EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,	)	
Plaintiff and Counterclaim-Defendant,	)	
v.	)	C. A. No.: 04-1199 (SLR)
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation,	)	
Defendants and Counterclaim-Plaintiffs.	)	

EXPERT REPORT OF DANIEL TEAL

TABLE OF CONTENTS

I. INTRODUCTION

1. I, Daniel M. Teal, am the Co-Founder and President of CoreTrace Corporation, a computer security corporation that specializes in providing scalable, secure, Enterprise Computing Management (ECM) systems.

2. I have been retained by counsel for Symantec Corporation as an expert witness in this action. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

II. QUALIFICATIONS

3. I received a Bachelor of Science degree in Electrical Engineering from the Massachusetts Institute of Technology in 1989. I undertook additional computer-related graduate work at the University of Texas at San Antonio from 1992 – 1994.

4. I was the Co-Founder and Chief Scientist of the WheelGroup Corporation (WheelGroup). Beginning in December 1995 – March 1998, WheelGroup designed and implemented the NetRanger Security Management System, one of the first network-based intrusion detection systems. WheelGroup was acquired by Cisco Systems, Inc. in March 1998 for $124 million in stock. From March 1998 – August 1999 I served as a senior software engineer for Cisco Systems, Inc., where I was responsible for research and development tasks to enhance the network security product line including the NetRanger product.

5. At the WheelGroup, I was both the main system architect and the primary software engineer/developer for the initial versions of the NetRanger product. In particular, I wrote the NSX and communications components of the software. I also wrote the majority of the Director software with the exception of the interface with HP Openview network management software. By version 2.0 of NetRanger, the WheelGroup had added additional software developers, but I still served as the primary architect and developer.

6. Prior to my work at WheelGroup, I served as an Officer in the United States Air Force from October 1989 – November 1994, and worked in a variety of positions where my duties and responsibilities included protecting the networks and computer systems of the U.S. Air Force from potential intruders. In particular, from October 1993 – October 1994, I was the Air Force program manager, senior technical engineer, and system architect for the Distributed Intrusion Detection System (DIDS) – a real-time system for detecting and monitoring intrusion attempts against Air Force computer networks by outside attackers and malicious internal users.

7. A more detailed summary of my professional experience is attached as Exhibit A.

8. I receive compensation in the amount of $250.00 per hour for the time that I devote to this matter. My compensation is not dependent in any way on the outcome of this matter.

III. METHODOLOGY AND BASES

9. In preparing my opinions and analysis of the art, I have thoroughly reviewed the entire specification and claims of U.S. Patents No. 6,321,338 (the '338 patent); 6,484,203 (the '203 patent); 6,708,212 (the '212 patent); and 6,711,615 (the '615 patent) (collectively, the patents-in-suit). I have also reviewed each of the prosecution histories associated with the patents-in-suit.

10. I understand that the Court has not yet construed certain claim terms of the claims of the patents-in-suit. Since the Court has not yet issued a decision construing the claims of the patents-in-suit, I have been asked, for purposes of this analysis, to assume that the Court adopts the claim construction positions advanced by SRI. I have reviewed a copy of the Joint Claim Construction Statement which includes SRI's positions on certain terms. For certain terms discussed in this report, no construction has been offered by any party. In such cases, I have been asked to use the ordinary meaning of that term.

I understand that claim language is generally construed in accordance with its ordinary and customary meaning to those skilled in the relevant art as of the date of the invention.[1] I also understand that claim terms should be given the meaning that is objectively discerned from the specification and/or the prosecution history by one of ordinary skill in the art as of the date of the invention, even if that meaning differs from the term's ordinary and customary meaning.

11. I have reviewed an extensive body of prior art publications as well as certain embodiments of the NetRanger software. A list of the prior art publications, documentation, and software embodiments I have reviewed and the individuals with whom I have spoken in forming the opinions set forth below is attached as Exhibit B. Exhibit B also lists the Bates ranges for each document discussed in this report, which I understand designates the version of the document produced in this litigation.

IV. NETRANGER DOCUMENTATION PUBLICLY AVAILABLE PRIOR TO NOV. 9, 1997

12. The NetRanger Security Management System, ("NetRanger") was and is a real-time network security management system for detecting, analyzing, responding to, and deterring unauthorized network activity. Versions of NetRanger have been available commercially since 1996.

13. As a co-founder and past Chief Scientist of the WheelGroup which created NetRanger, I have first-hand knowledge of the functionality of successive NetRanger

[1] "As a starting point, we give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art. ... Accordingly, a technical term used in a patent is interpreted as having the meaning a person of ordinary skill in the field of the invention would understand it to mean." *Bell Atlantics Network Servs., Inc. v. Covad Comm. Group, Inc.*, 262 F.3d 1258, 1267-268 (Fed. Cir. 2001). *See also Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc).

product embodiments as well as the documentation, presentations, and press releases prepared by WheelGroup and others about NetRanger. In addition, I maintained detailed files of product descriptions and documentation from December 1995, when I first began working on NetRanger, through March 1998, when the product was sold to Cisco Systems. In order to ensure that my recollection of the details of each of the NetRanger versions discussed below was correct, and that my recollection of the dates of the release of each of the documents listed below was correct, I searched my own personal files to find copies of various press releases, presentations, User Guides and Manuals, and other documentation developed by WheelGroup and others. In addition, I spoke to former WheelGroup colleagues Scott Olson, Scott Waddell, Kevin Wiley, and Jerry Lathem to further verify that my recollection of past events was correct. I also reviewed archived versions of the WheelGroup website (www.wheelgroup.com) from the Internet Archive to further confirm my recollection of when certain documents were posted to the WheelGroup website.

A. NetRanger User Guides and other software manuals

1. NetRanger User's Guide Version 1.3.1

14. The NetRanger User's Guide Version 1.3.1 [SYM_P_0074948-SYM_P_0075282] was publicly available prior to August 25, 1997. The document itself is marked "Copyright © 1997 WheelGroup Corporation." Furthermore, version 1.3.1 of NetRanger was released prior to version 2.0, and an official WheelGroup press release from my files indicates that WheelGroup released version 2.0 on August 25, 1997. [SYM_P_0074722-SYM_P_0074723].

15. This User's Guide was provided along with each sale of the NetRanger product version 1.3.1. In addition, if asked by a potential customer the WheelGroup provided copies of their user manuals upon request. NetRanger version 1.3.1 was sold commercially by WheelGroup. WheelGroup customers who purchased the system

include the US Air Force, IBM, AT&T, Storage Tek, NetSolve, Network General, and BTG. Attached at Exhibit C is a WheelGroup customer list identifying the companies that purchased different versions of NetRanger.

2. NetRanger User's Guides (earlier versions)

16. Each of the following versions of the NetRanger User's Guide were also available publicly prior to August 25, 1997, and were provided along with each sale of the NetRanger product of the same version:

- NetRanger User's Guide, WheelGroup Corporation, 1996. [SYM_P_0526566-SYM_P_0526735]
- NetRanger High-Level Overview, Version 1.1, WheelGroup Corporation, 11/1996 [SYM_P_0531123- SYM_P_0531139].
- NetRanger User's Guide Version 1.2.2, WheelGroup Corporation, 1997 [SYM_P_0075283- SYM_P_0075535].
- NetRanger User's Guide Version 1.2, WheelGroup Corporation, 1997 [SYM_P_0071736- SYM_P_0071953].

3. Data Privacy Facility / BorderGuard

17. The NetRanger product was designed to work with the NSG BorderGuard security device, which provided virtual private network (VPN) capabilities for NetRanger communications. The Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 [SYM_P_0072419- SYM_P_0072641] explains the cryptographic component of the BorderGuard security device. This document was publicly available as of September 1995, when it was provided along with each NSG BorderGuard security device sold commercially. In addition, as indicated at page iii of the DPF Version 1.2 Guide, both a Reference Manual and an Installation Guide were also available for the BorderGuard router itself as of September 1995. Exhibit B contains a list of additional BorderGuard manuals that were publicly available prior to November

1997. Documentation from the Internet Archive from www.network.com [SYM_P_0600799-0600839] further confirms my recollection that multiple versions of the BorderGuard router were publicly available prior to November 1997.

4. HP OpenView

18. The NetRanger product was also designed to operate in conjunction with HP OpenView. HP OpenView was a very well-known network management software application. Up until late 1997, all NetRanger customers were required to purchase a copy of HP OpenView. (NetRanger eventually supported customers using the IBM Netview application as well, and later developed a NetRanger user interface instead of requiring customers to purchase HP OpenView). Thus, I am generally familiar with the sales and marketing of HP OpenView in the 1996-1998 timeframe. Although NetRanger ran on the Unix version of HP Openview, I believe that the major functionality of HP OpenView was similar between the Unix and Windows versions. I know that the HP OpenView product was sold with user manuals, and I would expect that the HP OpenView for Windows User Guide Version 6.1 for Windows [SYM_P_0080944-SYM_P_0081098] would have been publicly available with HP OpenView products as of the October 1997 date indicated in this manual.

B. NetRanger Slides

19. In addition to selling the NetRanger product itself and associated documentation, the WheelGroup also provided training seminars to train customers and potential customers on how to set up and use NetRanger. In April 1997, the "NetRanger Installation & Configuration Training" slide presentation consisted of the documents at [SYM_P_0077338- SYM_P_0077416]. These slides were publicly shown to customers beginning in April 1997. These training sessions were open to any customer who signed up for one of the multiple sessions offered per year. Customers receiving training include the US Navy (May 1997), AT&T (May 1997), American Express (Sept. 1997), and IBM

(Aug. 1997). Each of these customers was shown the "NetRanger Installation & Configuration Training" slide presentation.

C. SQL Queries

20. The SQL queries given at [SYM_P_0074926- SYM_P_0074947] were publicly available as of May 28, 1997. The functionality of these SQL queries was also described, for example, in the NetRanger User's Guide Version 1.3.1 at p. 5-36 [SYM_P_0075174]. These SQL queries were included in source form with the NetRanger product starting with version 1.2. All NetRanger customers of version 1.2 and later could have viewed these SQL queries as part of the NetRanger product that they purchased.

D. DoD Spock Report

21. In March 1997, a Department of Defense-sponsored consortium of both government and commercial organizations performed a detailed evaluation of the capabilities of the NetRanger product. This group, including the National Security Agency, was known as the Security Proof of Concept Keystone (SPOCK). The results of the SPOCK evaluation were documented in a detailed report entitled "NetRanger Real-Time Network Intrusion Detection Performance and Security Test," DoD/SPOCK, including Appendices A, B and C, 4/30/1997 [SYM_P_0074255- SYM_P_0074481].

22. On July 8, 1997 the WheelGroup issued a press release entitled "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger intrusion detection system." [SYM_P_0074647-SYM_P_0074648; SYM_P_0074525-SYM_P_0074526]. As part of this press release, the WheelGroup notified the public that the underlying report documenting the SPOCK evaluation could be obtained by writing to COACT, Inc. 9140 Guilford Road, Suite L, Columbia, MD 21046. Thus despite the SPOCK report being marked "For Official Use Only" the document was made available to members of the public upon request and is therefore not confidential. See also Minutes of SPOCK

meeting, 12/12/96, noting "the resulting test will be made available to all requesters." [SYM_P_0074461].

E. AFIWC Assessment

23. From October to December of 1996, the Air Force Information Warfare Center (AFIWC) performed an extensive test of two different NetRanger configurations. The resulting report was entitled "Product Security Assessment of the NetRanger Intrusion Detection Management System Version 1.1," AF Information Warfare Center, February, 1997 [SYM_P_0074527- SYM_P_0074566].

24. It is my understanding that this report was not classified and was available via Freedom of Information Act (FOIA) requests. The WheelGroup had multiple internal copies of this document and it was not treated as confidential. This report was certainly available to government customers of NetRanger as well.

F. WheelGroup Press Releases

25. The WheelGroup made periodic press releases to inform the public about its products, including NetRanger. These press releases were published on the company's website at www.wheelgroup.com. A summary of when each press release was posted is given in "WheelGroup Press Release Summary" [SYM_P_0074525 SYM_P_0074526].

26. In particular, the press release entitled "WheelGroup Releases NetRanger Version 2.0" was published on the WheelGroup website on August 25, 1997. [SYM_P_0074722-SYM_P_0074723]. In addition, the press release entitled "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger intrusion detection system" was published on the WheelGroup website on July 8, 1997. [SYM_P_0074647-SYM_P_0074648].

V. FUNCTIONALITY OF THE NETRANGER PRODUCT AS OF NOV. 9, 1997

27. The NetRanger product as of November 1997 was a well-developed commercial product that had already undergone several different version upgrades to enhance its feature set and functionality. NetRanger was a network security management system capable of operating in real time, which meant that potential intrusions and suspicious activity were detected on the fly, as traffic flowed through the network being monitored. NetRanger operated in TCP/IP networks and could function in a distributed fashion across large networks or multiple sites interacting across the Internet.

28. NetRanger was designed to work with other commercially-available products, such as the BorderGuard security device, and both the HP OpenView and IBM NetView network management systems.

29. The BorderGuard product from Network Systems Corporation circa 1997 was a router / packet filter that was capable of filtering a full set of protocols, including but not limited to the IP protocol. BorderGuard also included sophisticated encryption and VPN capabilities, allowing traffic to be passed securely even over the Internet.

30. NetRanger also integrated with and required the functionality of certain network management systems. Network management systems were used to manage and properly display the data collected from NetRanger sensors. NetRanger required a user to purchase either HP OpenView or IBM NetView in order to use the Director functions of NetRanger.

31. The basic NetRanger system was composed of three main "core" systems that interacted to detect, analyze, respond to and deter unauthorized network activity: the NSX, the Communication System, and the Director.

32. The Network Security eXchange (NSX) system included a Packet Filtering Device subsystem and a Sensor subsystem, and provided the capability to capture network traffic and analyze it to detect suspicious activity. The Packet Filtering

Device component plugged into a network as a router or a bridge, and routed network traffic to the Sensor. The Sensor component contained NetRanger's real-time intrusion detection and content assessment logic. The Sensor's intrusion detection engine contained a large set of different rules, or signatures, capable of detecting a wide assortment of attacks such as sendmail attacks, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN attacks. Sensor analyses produced event records of detected attacks and alarms which were automatically sent on to a Director.[2] The Sensor also accepted intrusion response and reconfiguration information from a Director. An individual NSX could communicate with more than one Director if desired.

33. The NetRanger Communication System included the so-called "post office" subsystem and an Encrypted Sleeve. The post office provided a communication backbone for remote monitoring and transmission of information between the NSX and the Director. The Encrypted Sleeve provided secure data transmission between remote networks and the various NetRanger components by creating a virtual private network (VPN) between each component using the Data Privacy Facility (DPF) that came with Network Systems Corporation's BorderGuard devices. As noted previously, NetRanger was designed to operate in conjunction with the BorderGuard security device. The BorderGuard security device could be installed in various different places on the network being monitored.

34. The Director provided integration and analysis services to NetRanger, and communicated with one or more NSXs via the communication system. The Director included two subsystems, the Security Management Interface (SMI) and the Security Analysis Package (SAP). The SMI subsystem integrated with network management software to provide a graphical user interface (GUI) and tools to assist a user in monitoring and responding to security events occurring on different NSXs reporting to

[2] The NetRanger documentation uses the terms "event" and "alarm" interchangeably, as do I.

that Director. The SAP subsystem provided additional data management, data analysis capabilities, and the ability to generate reports correlating information from multiple sources. The SAP subsystem could be configured to run on the same platform as the SMI, or run on a separate database server.

35. NetRanger used the BorderGuard security device to copy packets directly off the network and send them to the NSX Sensor for analysis. The BorderGuard device could be configured to send all packets to the Sensor, or a defined subset of the packets. NetRanger included a large variety of signatures to analyze the packets, some of which looked at the structure of the packet headers, and some of which looked at the data being transported in the packet.

36. Different NetRanger signatures indicate that NetRanger monitored at least the following different "categories" of network traffic. These categories of network traffic are called out in '203 patent claim 1 and '615 patent claim 1:

Claimed category	**Monitored**
network packet data transfer commands	• FTP directories created/deleted (4-79) • FTP files GET/PUT (4-79) • HTTP GET (4-80)
network packet data transfer errors[3]	• IP fragments (4-61) • ICMP unreachable (4-67) • ICMP parameter problem on datagram (4-69) • Failed FTP attempt (4-82)
network packet data volume	• ICMP flood (4-61) • Large ICMP traffic (4-63) • ICMP network sweep (4-63) • TCP port sweep (4-63) • UDP port scan (4-63) • SATAN scan (4-63) • Number of bytes within a TCP connection (4-72)
network connection requests[4]	• Connection request from specific IP address (1-10) • TCP connection requests (SYN packets) (4-63) • Connection requests from various other network

[3] Some of these errors, including "ICMP unreachable" would also constitute "an error code indicating a reason a packet was rejected" as claimed in '338 claim 10.

Claimed category	Monitored
	services (C-4 to C-5) • Failed logins (FTP, telnet and rlogin authentication failures)
network connection denials	• FIN packets (4-72) • RST packets (4-72) • Failed logins (FTP, Telnet, rlogin authentication failure (4-62)
error codes included in a network packet	• multiple types of failed packets and connections (4-82) including failed ping and finger requests
network packets indicative of well-known network-service protocols	• unknown IP protocol (4-61)

37. A fundamental design principle of NetRanger was its modularity. Each of the different services required for the various subsystems were broken apart into their atomic operational components, or daemons. This approach allowed for improved speed, durability, scalability, and independence.

38. NetRanger was also perfectly suited for use in distributed, hierarchical monitoring. As shown in the attached Figure 1 in Exhibit D a single NSX could communicate with more than one Director. In addition, Directors could be configured into a hierarchy of Directors, where more than one Director reported up to a higher-tier Director. As shown in the attached Figure 2 in Exhibit D, the WheelGroup in its training slides explained to customers that NetRanger could operate in a four-tier hierarchy, with the NSX sensors serving at the lowest level collecting and analyzing network traffic. Events from these NSXs would be passed to a set of Directors at Tier 3 providing local network security management. A desired set of events, or all events, depending on user preferences, could also be passed up to a smaller set of Directors at Tier 2, which would consolidate information across multiple local Directors and provide regional management. Finally, regional Directors could pass information to a single overall

[4] The NetRanger software included a TCP stream reassembly engine used for many of the NetRanger signatures. This engine would monitor network connections using "a correlation of network connections requests and network connection denials" as claimed in '338 claim 7.

Director at Tier 1, which would further consolidate information and provide enterprise-level management.

39. In the spring of 1997, the DoD/SPOCK analysis was performed to test the capabilities of the NetRanger system. NetRanger was tested in an operational environment over a seven site network connected via an Internet based virtual wide area network (WAN). The WAN was comprised of Internet connections between the following sites: Army Battle Command Battle Laboratory (BCBL) at Fort Gordon, Georgia; NSA/V2 at Fort Meade, Maryland; Air Force Information Warfare Center in San Antonio, Texas, Center for Integrated Intelligence Systems (Space and Naval Warfare Systems Command) in McLean Virginia, Fleet Information Warfare Center, Norfolk, Virginia, and Land Information Warfare Activity, Fort Belvoir, Virginia. An NSX and a Director was placed at each of these sites. In addition, a Director was placed at COACT Inc. (NSA) in Columbia Maryland, to provide global monitoring at all sites.

40. NetRanger also provided automatic integration and correlation of event/alarm data generated from the analysis of network traffic. The Director automatically integrated multiple alarms in certain situations to reduce and consolidate the amount of data presented at the Director level. For example, a TCP port sweep over a variety of source-destination port pairs would be integrated into a single alarm icon. Not every packet received would be used to generate an Alarm icon on the Director – the alarm had to exceed a defined severity threshold. Furthermore, if two or more alarms were received that were similar in all respects except for their timestamp and alarm identification number, the Director would consolidate these multiple alarms into a single "Alarm set" icon.

41. Detection of a SATAN attack also required NetRanger to correlate different events to determine that indeed a SATAN attack was occurring. The NetRanger Sensor would recognize and track multiple different events occurring at different times, such as a ping sweep alarm and a later port sweep. The NSX would keep track of these

multiple different events as they occurred, and when appropriate would generate a SATAN attack event based upon the correlation of the occurrence of these events.

42. The NetRanger Director SAP subsystem also provided automatic correlation of event data. SAP was shipped with a set of comprehensive SQL queries to analyze data based upon different perspectives. These queries could be customized to automatically run periodically and generate different reports of events. For example, the Space Dimension queries would correlate events based upon where the attacks came from, allowing a user to see, for example, the "top ten addresses generating attacks" on the system being monitored. The Time Dimension queries would correlate events based upon when events occurred. The Events Dimension queries would correlate events by linking related attack types and related alarm severity levels.

43. I currently have a working version of the NetRanger 2.1 product in binary form. The 2.1 version of NetRanger, released in January 1998, was functionally identical to NetRanger Version 2.0 in all relevant aspects. The only differences were the additional of more attack signatures, and some minor bug fixes. At trial, I may rely upon this code or a similar version to demonstrate the relevant features of the NetRanger product.

VI. COMMERCIAL SUCCESS OF NETRANGER

44. Commercial intrusion detection systems first began to appear in the 1990s. It is often difficult to cleanly distinguish between a network intrusion detection system and many other network systems that perform some type of security function, such as network monitoring and management software, or the wide variety of firewalls in existence in the 1990s. Nevertheless, I think it is fair to say that the WheelGroup, founded in 1995, was one of the first companies to develop a commercially viable network intrusion detection system. WheelGroup's primary competitor in the market in the 1996-1997 timeframe was the ISS RealSecure product.

45. Sales of NetRanger were good. WheelGroup customers include the US Air Force, US Navy, IBM, AT&T, Storege Tek, Network General, BTG, Perot Systems, Alcatel, CDW, Boeing, Procter and Gamble, Citibank, CompuServ, Chrysler, Allstate, and many others. A WheelGroup customer list dated January 5, 1998 lists 65 customers using NetRanger. Twenty of those companies were in the Fortune 500.

46. Commercial partners of WheelGroup also used NetRanger in services offerings to their customers. Such companies would use the NetRanger product to monitor their customer's network, typically with a Director back at the service company's headquarters to provide real-time monitoring of each customer's network. For example, the ProWatch Secure service offered 24-hour monitoring of traffic on Internet gateways using NetRanger. IBM network services also purchased NetRanger for use as a monitor/sensor in their service offerings.

47. In addition to commercial sales to customers, the NetRanger product was also purchased and used by the U.S. Government. For example, in approximately July 1996, the 609th Information Warfare Squadron located at Shaw Air Force Base (AFB) spent approximately $800k to purchase the NetRanger system to protect US Air Force computer networks.

48. Eventually in March 1998, Cisco Systems Inc. purchased the entire WheelGroup Corp., including the NetRanger product line, for $124 million in stock. Cisco's primary reason for purchasing WheelGroup was its desire to obtain the NetRanger product in order to have a commercially viable network intrusion detection offering, which helped round out Cisco's other networking product offerings. This sale of the company to Cisco demonstrates the desirability and commercial success of the NetRanger product. Cisco changed the name of the product to the "Cisco Secure Intrusion Detection System" for marketing reasons. NetRanger code and technology is still used in the product today and many of WheelGroup's software developers are still employed by Cisco to continually improve the product.

49. I believe that the WheelGroup NetRanger product was successful for two reasons: the product worked as advertised and it was very reliable. NetRanger successfully passed operational tests time and time again by reliably detecting network attacks. It was able to operate continuously over a period of months without crashing. I remember that some of our customers, including IBM ERS, purchased NetRanger after they had already purchased the ISS RealSecure product because our system was so reliable.

VII. LACK OF NOVELTY

50. I understand that a patent is not valid if it can be shown by clear and convincing evidence that the inventions disclosed in the patent are not new and novel. An invention is not novel if the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States.[5] The effective filing date for all of the patents-in-suit is November 9, 1998.

51. In order to demonstrate a lack of novelty, an invalidating prior art reference must disclose each and every limitation of the claimed invention, either expressly or inherently, in detail sufficient to enable one of ordinary skill in the art to practice the claimed invention without undue experimentation. For the purpose of this analysis, I was asked to assume that one of ordinary skill in the art in 1997 would have been someone with an undergraduate degree in Computer Science with at least three to five years experience in computer programming and network design with an emphasis in network monitoring technology and intrusion detection.

52. As shown in the chart attached as Exhibit E, it is my opinion that the NetRanger User's Guide Version 1.3.1 is a printed publication prior art reference that invalidates claims 1-22 of U.S. Pat. No. 6,484,203 and claims 1-6, 8-23, 34-53, 64-73,

[5] 35 U.S.C. sec 102(b).

and 84-93 of U.S. Pat. No. 6,711,615. In addition, as shown in the same chart, the NetRanger product itself circa November 9, 1997 also demonstrates that the alleged inventions described in these claims were in public use and on sale more than one year prior to the date of application for these patents.

VIII. OBVIOUSNESS

53. In addition to the requirement that a patent claim be novel, I understand that a patent claim is presumed valid unless it is shown by clear and convincing evidence that the differences between the subject matter claimed and the prior art were such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains.[6]

54. I understand that in determining the obviousness of the claim(s) of a patent, one should consider:

a. the scope and content of the prior art relied upon by the party alleging invalidity of the patent;

b. the differences, if any, between each claim of the patent and the prior art; and

c. the level of ordinary skill in the pertinent art at the time the invention of the patent was made; and

d. whether the prior art enabled a person of ordinary skill in the art to make and use the invention claimed.

55. I understand that one must also consider such objective considerations as commercial success, long-felt but unresolved need, failure of others to solve the problem, acquiescence in the patent by others, and whether the same or similar inventions were made independently by others prior to or at about the same time as the invention claimed in the patent.

56. I understand that the test of obviousness is whether the claimed invention, as a whole, would have been obvious to one of ordinary skill in the art as of the date of

[6] 35 U.S.C. sec 103.

the invention in light of the prior art. To establish obviousness under this test, I understand that one must show by clear and convincing evidence that a person of ordinary skill in the art at the time of invention, confronted by the same problem as the inventor and with no knowledge of the claimed invention, would select the recited elements from the prior art and combine them in the claimed manner. In other words, one must avoid the use of hindsight and instead identify in the art prior to the invention some suggestion or motivation, before the invention itself was made, to make the new combination.

57. I understand that the motivation to combine prior art references need not be expressly stated in the prior art, but that it may be found, for example, in the nature of the problem to be solved, or may come from the knowledge of those skilled in the art.

58. As described previously, the NetRanger NSX component correlated different attack signatures to determine whether or not a SATAN attack was occurring. It would have been obvious to perform this correlation at the Director as well. One of skill in the art would have been motivated to make this minor change in order to facilitate detecting a SATAN attack occurring across multiple NSX sensors.

59. The NetRanger system looked for patterns in network traffic indicative of known attacks. However, it was well-known in the intrusion detection field at the time that one might also monitor a network to try and detect behavior that appeared anomalous, or different, from the normal behavior of the network. Often referred to as "anomaly detection," these methods were supposed to be able to detect unknown attacks that deviated from normal activity but did not match any known attack pattern.

60. The use of statistical profiling for performing anomaly detection was well-known by November 9, 1997. By that time, SRI had published extensively on the use of statistical profiling in NIDES (Next-generation Intrusion Detection Expert System).[7] SRI

[7] *See, e.g.*, A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next Generation Intrusion Detection Expert

had also published on the EMERALD system.[8] It had been suggested by many researchers in the field at the time that it was desirable to combine both signature-based detection to look for known attacks with anomaly detection to look for potentially unknown attacks. Thus, it would have been obvious to one of ordinary skill at the time to combine a statistical profiling method for anomaly detection such as those described in *Statistical Methods* and *Emerald 1997* with the NetRanger system if commercial-grade software implementing such an anomaly detection system had existed in 1997. Therefore, as indicated in the chart in Exhibit E, U.S. Patent 6,711,615 claim 7 and claims 1-24 of U.S. Patent 6,708,212 are invalid as obvious.

61. However, the needs of a commercial system such as NetRanger were very different than a research system. In particular, when performing real-time network intrusion detection, it was of paramount importance that the software analyzing the network traffic run quickly in order to be able to keep up with the incoming stream of network packets. WheelGroup actually investigated adding such statistical anomaly detection functionality to NetRanger, and based upon our investigation I do not believe a commercial-grade system for statistical anomaly detection existed in 1997 that was suitable for inclusion in NetRanger. However, since we actually considered adding such functionality to NetRanger back in the 1996-1997 timeframe, I believe it would have been obvious to combine NetRanger with a statistical anomaly detection system if one's primary purpose was the creation of a research-oriented system, as opposed to a commercial product.

System)", January 27, 1995 ("*Statistical Methods*") [SYM_P_0068937-SYM_P_0068942].

[8] *See, e.g.*, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Oct. 9, 1997 ("*Emerald 1997*") [SYM_P_0535485 – SYM_P_0535497].

IX. ASIM

62. I helped setup the first monitoring systems for the US Air Force Automated Security Incident Management (ASIM) program. We implemented the first monitoring sites by using the Network Security Monitor (NSM) developed by Todd Heberlein at UC Davis. Initial sites included the Air Force 7th Communications Group located at the Pentagon in Washington D.C. and Wright-Patterson AFB located in Dayton, OH. Both sites were fully operational by the end of 1992. We installed the NSM software on Sun SPARCstations attached to operational Air Force networks. The NSM software at the time included several different types of analysis engines for analyzing network traffic. However, we focused our operations on utilizing NSM's capability to detect specific strings of text within TCP and UDP network sessions. Samples of strings include "login: root" and "GET passwd." Although these examples may seem trivial compared to a modern IDS, they were very effective in detecting unauthorized use of Air Force networks. The success of these early monitoring systems help spur the development of better technologies and operational procedures at the Air Force Information Warfare Center (AFIWC).

Dated: April 19, 2006

Daniel M Teal

Daniel M. Teal

Exhibit A

Professional Experience:

5/00 – Present	Co-Founder and President, CoreTrace Corporation, Austin, TX
	Doing research and development for a next generation host and network security system.
7/99 – Present	Private investor, philanthropist, advisor.
3/98 – 7/99	Senior Software Engineer, Cisco Systems, Austin, TX
	Responsible for research and development tasks to enhance network security product line including the Cisco NetRanger Security Management System.
12/95 – 3/98	Co-Founder and Chief Scientist, WheelGroup Corporation, San Antonio, TX
	One of the founders of WheelGroup Corporation. Designed and implemented the NetRanger Security Management System. Responsible for leading development of information security software. WheelGroup Corporation was acquired by Cisco Systems, Inc. in March 1998 for $124 million in stock.
11/94 - 12/95	Senior Engineer, Trident Data Systems, San Antonio, TX
	Analyzed security vulnerabilities in operating systems and network protocols for developing information security software. Performed security posture assessments of customer networks.
10/89 – 11/94	Officer, USAF
	Received commission as 2nd Lt upon graduation from MIT via 4yr ROTC program. Honorably discharged in November 1994 with rank of Captain.
10/93 - 10/94	Network Security Engineer, Air Force Information Warfare Center, Kelly AFB, TX
	Responsible for the research, design, development, and deployment of sensitive countermeasures for Air Force networks and computer systems. Air Force program manager, senior technical engineer, and system architect for the Distributed Intrusion Detection System (DIDS) - a real-time system for detecting and monitoring intrusion attempts against Air Force computer networks by outside attackers and malicious internal users
2/90 - 9/93	Systems Security Engineer, Air Force Cryptologic Support Center, Kelly AFB, TX
	Analyzed the vulnerabilities of essential Air Force networks to current threats and developed specific countermeasures. Technical security consultant to Air Force organizations. Responded to foreign attacks against Air Force systems. Designed architecture for automated security posture measurement of Air Force systems.
6/89 - 10/89	Technical Consultant, John Deere Horicon Works, Horicon, WI
2/88 - 5/89	Researcher, MIT Sloan School of Management, Cambridge, MA
6/88 - 5/89	Researcher, MIT Flight Transportation Laboratory, Cambridge, MA
8/87 - 1/88	Researcher, MIT Laboratory for Information Systems, Cambridge, MA

Education:

Graduate	University of Texas at San Antonio, San Antonio, TX Specialized Graduate courses, Sep 1992 to Jan 1994	GPA: 4.0/4.0
Undergraduate	Massachusetts Institute of Technology, Cambridge, MA Bachelor of Science in Electrical Engineering, June 1989	GPA: 4.0/5.0

Exhibit B

I. NetRanger documentation

User Manuals

- NetRanger User's Guide, WheelGroup Corporation, 1996. [SYM_P_0526566-SYM_P_0526735]
- NetRanger High-Level Overview, Version 1.1, WheelGroup Corporation, 11/1996 [SYM_P_0531123- SYM_P_0531139].
- NetRanger User's Guide Version 1.2.2, WheelGroup Corporation, 1997 [SYM_P_0075283- SYM_P_0075535].
- NetRanger User's Guide Version 1.2, WheelGroup Corporation, 1997 [SYM_P_0071736- SYM_P_0071953].
- NetRanger User's Guide Version 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948- SYM_P_0075282].
- NetRanger User's Guide Version 2.1.1, Cisco Systems, Inc., 1998 [SYM_P_0068166- SYM_P_0068499].
- Release Notes for NetRanger 2.1.1, Cisco Systems, Inc., 1998 [SYM_P_0068500-SYM_P_0068539].

Government test materials

- "NetRanger Real-Time Network Intrusion Detection Performance and Security Test," DoD/SPOCK, including Appendices A, B and C, 4/30/1997 [SYM_P_0074255- SYM_P_0074481].
- Product Security Assessment of the NetRanger Intrusion Detection Management System Version 1.1, AF Information Warfare Center, 2/1997 [SYM_P_0074527-SYM_P_0074566].

NetRanger code

- NetRanger SQL queries, 5/28/1997 [SYM_P_0074926- SYM_P_0074947].
- NetRanger 2.1 binary

NetRanger presentations

- NetRanger training slide presentations, 4/1997 [SYM_P_0077338-SYM_P_0077416].

- Networkers Active Audit – Scanning, and Intrusion Detection, Cisco US Networkers '98, 6/16/1998 [SYM_P_0068540- SYM_P_0068559].

Press / Press Releases

- R. Power and R. Farrow, "Detecting Network Intruders," Network Magazine, pp. 137-38, October 1997 [SYM_P_0078627- SYM_P_0078630].

- PC Week, "NetRanger keeps watch over security leaks," 9/1/97 [SYM_P_0077928- SYM_P_0077931].

- "WheelGroup Releases NetRanger Version 2.0," WheelGroup press release, 8/25/1997 [SYM_P_0074722- SYM_P_0074723].

- "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger Intrusion Detection System," WheelGroup press release, 7/8/1997 [SYM_P_0074647-SYM_P_0074648].

- WheelGroup Press Release Summary [SYM_P_0074525 SYM_P_0074526].

Internet Archive pages from WheelGroup website

- WheelGroup.com Internet Archive documentation [SYM_P_0599032-0599091]

H. Other documentation

- Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 [SYM_P_0072419- SYM_P_0072641].
- "BorderGuard" by Terry Parsons and Alan Hsu, ZD Internet Magazine, Feb. 1997, http://www.govisionmaster.com/dir_technology/firewalls/15Firewall.htm [SYM_P_0599031].
- BorderGuard Internet Archive documentation http://web.archive.org/web/19970501195615/http://www.network.com/ [SYM_P_0600799-0600839]

- The Security Router Getting Started Guide Release 2.0, NSC, 1995 [SYM_P_0601013-0601752]

- BorderGuard 1000 Reference Manual Release 4.0, NSC, 1996 [SYM_P_0601940-0602441]

- BorderGuard Troubleshooting Guide Release 4.0, NSC, 8/1996 [SYM_P_0602656-0602761]
- BorderGuard 1000 Release Notes Release 4.01, NSC, 2/1997 [SYM_P_0601753-0601939]
- NetSentry User Guide Release 4.0, NSC, 2/1997 [SYM_P_0602442-0602655]
- HP OpenView for Windows User Guide Version 6.1 for Windows, Oct. 1997 [SYM_P_0080944-1098]
- A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next Generation Intrusion Detection Expert System)", January 27, 1995 ("*Statistical Methods*") [SYM_P_0068937-942].
- "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Oct. 9, 1997 ("*Emerald 1997*") [SYM_P_0535485 – 497].
- U.S. Pat. Nos. 6,321,338, 6,484,203, 6,708,212, 6,711,615 and associated file histories [SYM_P_0071535-0071549], [SYM_P_0071550-0071563], [SYM_P_0071564-0071579], [SYM_P_0071580-0071598].
- Joint Claim Construction Statement, filed March 17, 2006

Spoke to the following individuals:

- Scott Olson,
- Scott Waddell,
- Kevin Wiley,
- Jerry Lathem, and
- Todd Heberlein

Wheelgroup Corporation															
Sales By Category and Month			The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc.												
	Invoice					Category				NSX		DEV			
Customer	Date	P.O. #	Invoice	Dollars	Category Total	Category	End User	P	S	MGT	Dir	SAP	Mat		
CyberSafe Corporation	1/16/1996	1	9601-0001	10,329		Consulting	Chrysler								
BTG	1/31/1996		9601-0002	2,700		Consulting	BTG								
BTG	2/29/1996		9602-0001	10,318		Consulting	BTG								
BTG	3/31/1996		9603-0001	72,688		Consulting	BTG								
BTG	5/31/1996		9605-0001	39,935		Consulting	BTG								
BTG	6/12/1996	SE970034	9606-0001	9,805		Consulting	BTG								
CyberSafe Corporation	6/19/1996	2	9606-0001	5,000		Consulting	Chrysler								
CyberSafe Corporation	6/19/1996	3	9606-0002	8,875		Consulting	Prudential								
BTG	6/30/1996		9606-0003	43,129		Consulting	BTG								
BTG	6/30/1996	0023 IC4I	9606-0004	5,469		Consulting	BTG								
IBM ISSC	7/30/1996	S0D10549 LJ	9607-0001	54,668		Consulting	IBM - ISSC Geoplex								
BTG	7/31/1996		9607-0002	46,398		Consulting	BTG								
BTG	7/31/1996	0024 IC4I	9607-0003	3,848		Consulting	BTG								
STK	8/16/1996		9608-0002	41,827		Consulting	NSC SPA								
BTG	8/31/1996	0024 IC4I	9608-0005	56,555		Consulting	BTG								
BTG	8/31/1996		9608-0006	24,800		Consulting	BTG								
Sprint	9/26/1996		9609-0003	24,000		Consulting	Sprint								
BTG	9/30/1996		9609-0004	18,950		Consulting	BTG								
BTG	9/30/1996	0036 IC4I	9609-0005	12,150		Consulting	BTG								
STK	10/24/1996		9610-0002	17,285		Consulting	NetVest - Keytronic SPA								
BTG	10/31/1996	0036 IC4I	9610-0003	48,492		Consulting	BTG								
BTG	10/31/1996		9610-0004	10,189		Consulting	BTG								
NetSolve	10/31/1996		9610-0005	2,724		Consulting	NetSolve								
BTG	11/30/1996	TASK 96-11-1	9611-0001	21,474		Consulting	BTG								
BTG	11/30/1996	0036 IC4I	9611-0003	4,961		Consulting	BTG								
BTG	12/31/1996	TASK 96-11-1	9612-0004	19,063		Consulting	BTG								
BTG	12/31/1996	0036 IC4I	9612-0005	13,770	629,400	Consulting	BTG								
NetSolve	11/30/1996		9611-0004	448		Mon Serv	NetSolve								
NetSolve	12/1/1996		9612-0001	643	1,090	Mon Serv	NetSolve								
BTG	8/29/1996	0034 IC4I	9608-0001	191,308		Product	AF - IWS	4					X		
BTG	8/29/1996	0035 IC4I	9608-0004	600,036		Product	AF - IWS	28			8		X		
NetSolve	9/3/1996	C-2175	9609-0001	28,281		Product	NetSolve	2							
NetSolve	9/12/1996	C-2193	9609-0002	25,874		Product	NetSolve	1							
NetSolve	10/15/1996	C-2193	9610-0001	18,996		Product	Gulf States Toyota	1							
NetSolve	11/19/1996		9611-0002	16,881		Product	NetSolve								
Network General Corporation	12/5/1996	72808	9612-0002	29,689		Product	Network Gen	1			1		X		
NetSolve	12/18/1996	I-4374	9612-0003	13,158	924,222	Product	DataWorks	1					X		
Total 1996				1,554,712	1,554,712			38			9	0			
Storage Technology Corp.	1/21/1997		9701-0001	40,425		Product	AT&T UGN	1			1	0			
STK	1/31/1997	51211	9701-0002	12,994	53,419	Product	BMC	1			1	0			
								2			2	0			
NetSolve	1/1/1997		9701-0003	700	700	Mon Serv									
BTG	1/31/1997		9701-0004	24,655	24,655	Consulting	BTG								
				78,774	78,774										
Storage Technology Corp.	2/12/1997		9702-0002	65,045		Consulting	STK SPA								
Lyondell Petrochemical	2/28/1997		9702-0007	82,856		Consulting	Lyondell								
BTG	2/28/1997		9702-0008	6,117	154,018	Consulting	BTG								
NetSolve	2/1/1997		9702-0006	895	895	Mon Serv									

EXHIBIT-C-1

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 31 of 109

Wheelgroup Corporation			The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..												
Sales By Category and Month															
	Invoice					Category				NSX		DEV			
Customer	Date	P.O. #	Invoice	Dollars	Total	Category	End User	P	S	MGT	Dir	SAP	Mat		
Network General Corporation	2/5/1997	73157	9702-0001	25,980		Product	Network Gen	4			0	0			
Storage Technology Corp.	2/20/1997		9702-0003	35,829		Product	AT&T Mesa	1			1	0	X		
Netsolve Incorporated	2/28/1997	I-4539	9702-0005	19,496	81,305	Product	BT Office Supply	1			0	0	X		
								6			1	0			
AT&T Wireless	2/25/1997	175475	9702-0004	3,874	3,874	Training	AT&T Wireless								
				240,092	240,092										
BTG	3/24/1997	0036 IC41	9703-0008	23,186		Consulting	BTG								
Tandem Computers	3/31/1997	3304910	9703-0011	11,800		Consulting	Tandem								
STK	3/31/1997		9703-0012	7,838		Consulting	AT&T Kansas City								
PCL Constructors Inc.	3/31/1997		9703-0013	8,600		Consulting	PCL								
BTG	3/31/1997		9703-0014	52,869	104,293	Consulting	BTG								
NetSolve	3/1/1997		9703-0003	895	895	Mon Serv									
STK	3/13/1997	51263	9703-0001	84,473		Product	CSE (Canadian equiv. of NSA	8			1	0			
STK	3/11/1997	29058	9703-0002	13,744		Product	NSC Internal	1			1	0			
STK	3/14/1997	51264	9703-0004	13,744		Product	NSC Internal	1			1	0			
NetSolve	3/14/1997	I-4583	9703-0005	19,496		Product	Computer Disc Warehouse	1			0	0	X		
STK	3/14/1997	51265	9703-0006	16,244		Product	NetCom Sol. S. Afr	1			1	0			
STK	3/21/1997	51290	9703-0007	25,991		Product	Citibank	2			1	0			
STK	3/26/1997	51304	9703-0009	21,991		Product	NSC Europe	2			1	0			
BTG	3/26/1997	971203	9703-0010	33,259	228,942	Product	BTG	1			1	1			
				334,131	334,131			17			7	1			
Quarter Total				652,996				25	0		10	1			
STK	4/30/1997		9704-0019	43,781		Consulting	Calif. Brd Equal.-Net 'Vest.								
BTG	4/30/1997		9704-0020	24,000	67,781	Consulting	Fiesta Crow,DARPA, etc.								
Various	4/30/1997		prepaid	13,000	13,000	Maintenance	Various								
NetSolve	4/1/1997		9704-0005	895		Mon Serv									
NetSolve	4/30/1997		9704-0017	948		Mon Serv	BTO								
NetSolve	4/30/1997		9704-0018	671	2,514	Mon Serv	CDW								
STK	4/8/1997	51320	9704-0004	18,798		Product	NSC Internal	2			0	1			
STK	4/22/1997	51342	9704-0007	16,673		Product	NSC Europe	2			0	0			
STK	4/22/1997	51338	9704-0008	15,976		Product	NSC U.K.	1			1	1			
STK	4/22/1997	51321	9704-0009	48,896		Product	NSC Japan	3			3	0			
NetSolve	4/22/1997	I-4696	9704-0010	15,145		Product	Structual Metals, Inc.	1			0	0	X		
STK	4/29/1997	27553	9704-0011	13,818		Product	NSC Internal	1			1	0			
STK	4/30/1997	51364	9704-0016	16,244		Product	Motorola	1			1	0			
STK	4/30/1997	51353	9704-0021	5,507	151,057	Product	STK	0			1	0			
								11			7	2			
Network General Corp.	4/15/1997		prepaid	50,000	50,000	Royalty	NGC								
EWA-Canada	4/30/1997	0465-C23-01/97	9704-0012	1,072		Training	EWA-Canada								
CANADIAN FORCES	4/30/1997		9704-0013	1,072		Training	Canadian Forces								
StorageTek Canada, Inc.	4/30/1997		9704-0014	1,608		Training	STK								
Storage Technology Corp.	4/30/1997		9704-0015	536	4,288	Training	STK								
				288,640	288,640										
CyberSafe Corp.	5/9/1997		9705-0004	54,900	54,900	Consult- ICR	CyberSafe Corp								
Various	5/31/1997		prepaid	13,000	13,000	Maintenance	Various								

EXHIBIT-C-2

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 32 of 109

Wheelgroup Corporation		The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..												
Sales By Category and Month														
	Invoice				Category				NSX		DEV			
Customer	Date	P.O. #	Invoice	Dollars	Total	Category	End User	P	S	MGT	Dir	SAP	Mnt	
NetSolve	5/9/1997		9705-0005	2,238	2,238	Mon Serv	Datasworks,CDW,BTO,SMI,GS Toyota							
STK	5/2/1997	51367	9705-0001	18,841		Product	Pilot Network Service	1			1	1		
STK	5/7/1997	51375	9705-0002	72		Product	STK Belgium	0			0	0		
STK	5/9/1997	51376	9705-0003	72		Product	STK Sweden	0			0	0		
NetCom Solutions	5/9/1997	97-131	9705-0006	22,995		Product	NetCom Solutions	2			1	0		
STK	5/13/1997	51386	9705-0007	6,507		Product	STK Canada	0			1	0		
BTG	5/22/1997	SE980094	9705-0008	128,956		Product	U.S. Navy	5			3	3		
NetSolve	5/20/1997	I-4901	9705-0013	19,635		Product	Texas Industries	1			0	0		
STK	5/30/1997	51348	9705-0014	18,767	215,845	Product	STK Colorado?	1			1	1		
								10			7	5		
BTG	5/22/1997		9705-0008	5,180		Training	U.S. Navy							
AT&T	5/28/1997	SPIL002332	9705-0009	2,085		Training	AT&T							
AT&T	5/28/1997	SPIL002263	9705-0010	2,085		Training	AT&T							
AT&T	5/28/1997	SPIL002264	9705-0011	1,390		Training	AT&T							
StorageTek	5/28/1997		9705-0012	1,943	12,683	Training	StorageTek							
				298,665	298,665									
Deloitte & Touche	6/16/1997		9706-0012	35,400		Consulting	Deloitte & Touche							
LVH	6/16/1997		9706-0014	35,400		Consulting	LVH							
Schrieber	6/16/1997		9706-0015	6,400		Consulting	Schrieber							
Harris Publishing	6/16/1997		9706-0013	6,400		Consulting	Harris Publishing							
Origin Systems	6/16/1997		9706-0016	6,400		Consulting	Origin Systems							
Enron	6/23/1997		9706-0020	5,000		Consulting	Enron							
Pictet & CIE	6/25/1997		9706-0022	6,400	101,400	Consulting	Pictet & CIE							
BTG	6/25/1997		9706-0023	4,200		Install	Ft. Huachuca							
NetSolve	6/30/1997		9706-0031	1,000	5,200	Install	SMI							
NetSolve	6/5/1997	M-4942	9706-0001	2,700	2,700	Maintenance	TXI							X
NetSolve	6/5/1997		9706-0002	2,238	2,238	Monitoring	TXI							
STK	6/11/1997	51414	9706-0005	15,942		Product	STK-Canada, EWA	1			1	1		
STK	6/11/1997	51423	9706-0006	18,841		Product	Aerospace	1			1	1		
STK	6/11/1997	51422	9706-0007	48,735		Product	BMC	5			0	0		
STK	6/11/1997	51431	9706-0008	18,841		Product	AT&T	1			1	1		
STK	6/11/1997	51421	9706-0009	32,435		Product	STK-Training	4			1	1		
STK	6/17/1997	51433	9706-0018	13,744		Product	STK-U.K.	1			1	0		
STK	6/27/1997	51438	9706-0024	28,588		Product	Lockheed	2			1	1		
Netsolve	6/27/1997	I-5044	9706-0025	19,496		Product	Corinthian Schools	1			0	0		
BTG	6/27/1997	SE980183	9706-0026	46,488		Product	Ft. Huachuca	2			1	0		
BTG	6/27/1997	SE980204	9706-0027	46,488		Product	BTG	2			1	0		
STK	6/28/1997	51442	9706-0028	18,841		Product	STK, France	1			1	1		
STK	6/30/1997	51446	9706-0029	16,244		Product	Boeing	1			1	0		
BTG	6/30/1997	SE980205	9706-0032	19,496		Product	BTG	1			0	0		
BTG	6/30/1997	SE980206	9706-0033	38,644		Product	Ft. Huachuca	1			1	0	X	
BTG	6/30/1997	SE980204	9706-0034	46,488		Product	BTG	2			1	0		
IBM	6/30/1997		9706-0035	51,980		Product	IBM-Eval units	1			1	1		
IBM-ERS	7/31/1997	2000241763	9706-0036	2,400	483,691	Product-Install	IBM-ERS							
								27			13	7		
maxiBIT GmbH	6/3/1997		9706-0004	1,295		Training	maxiBIT GmbH							
STK	6/9/1997		9706-0003	3,238		Training	STK							

EXHIBIT-C-3

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 33 of 109

Wheelgroup Corporation
Sales By Category and Month

The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..

Customer	Invoice Date	P.O. #	Invoice	Dollars	Category Total	Category	End User	NSX P	NSX S	DEV MGT	Dir	SAP	Mnt
BTG	6/27/1997		9706-0026	16,576		Training	Ft. Huachuca						
IBM-Global Services	6/30/1997	2000328910	9706-0030	2,590		Training	IBM-Global Services						
IBM-ERS	6/17/1997	2000241763	9706-0019	4,800	28,499	Training/Instal	IBM_ERS						
				623,727	623,727								
Second Quarter to Date				1,211,031				48			27	14	
BTG	7/14/1997		9707-0004	1,800	1,800	Consulting	Briefings (Fields, Mony, Navy, etc)						
STK	7/15/1997		9707-0009	17,886	17,886	Maintenance	Various						
Netsolve	7/1/1997		9707-0001	2,913	2,913	Monitoring							
STK	7/16/1997	51482	9707-0011	16,244		Product	CSX Technology	1			1	0	
STK	7/16/1997	51475	9707-0012	9,747		Product	All State Insurance	1			0	0	
Ernst & Young	7/25/1997	MIL617-2	9707-14-2	67,960		Product	Ernst & Young	2			1	1	X
STK	7/30/1997	51479	9707-0017	15,941		Product	Internal, MD	1			1	1	
STK	7/30/1997	51488	9707-0018	38,335		Product	Integrated Data Networks	3			1	1	
STK	7/30/1997	51495	9707-0019	18,841		Product	Internal, U.K.	1			1	1	
STK	7/30/1997	51478	9707-0020	19,494		Product	Internal, Canada	1			1	0	
IBM-ERS	7/30/1997	2000355028	9707-0021	89,568		Product	IBM-ERS	3			3	3	X
STK	7/30/1997	29425	9707-0022	9,747		Product	NetCom Sols, S.Af., EASCA	1			0	0	
STK	7/30/1997	29426	9707-0023	9,747		Product	NetCom Sols, S.Af., BMW	1			0	0	
STK	7/31/1997	51505	9707-0025	9,747		Product	NetCom, S.Af.	1			0	0	
Amex	7/31/1997	PHX080280	9707-0024	17,068	322,439	Product	Amex	0			1	1	X
								16			10	8	
Cemex	7/14/1997		9707-0003	34,000		Consulting	Cemex						
Openconnect Systems	7/14/1997	19678	9707-0006	28,400		Consulting	Openconnect Systems						
Fedex	7/14/1997		9707-0008	23,200		Consulting	Fedex						
Enron	7/14/1997		9707-0010	2,900	88,500	Consulting	Enron						
E-Systems	7/3/1997		9707-0002	1,295		Training	E-Systems						
STK	7/18/1997		9707-0013	1,295		Training	STK						
AT&T	7/25/1997	77811	9707-0014	1,295		Training	AT&T						
STK	7/25/1997		9707-0015	1,295		Training	STK						
Amex	7/31/1997		9707-0024	6,590		Training	Amex						
STK	7/31/1997		9707-0026	648		Training	STK						
UMI A.S.	7/31/1997		9707-0027	1,295		Training	UMI A.S.						
Hucom	7/31/1997		9707-0028	3,885	17,598	Training	Hucom						
				451,135	451,135								
Guidry	8/14/1997		9708-0011	3,375	3,375	Consulting	Iridium						
STK	8/14/1997		9708-0012	2,900	2,900	Installation							
NetSolve	8/1/1997		9708-0001	3,244	3,244	Monitoring	Various						
STK	8/15/1997	51501	9708-0014	16,244		Product	Korea Computer Tech.	1			1	0	
BTG	8/15/1997	SE980265	9708-0015	24,746		Product	Army JEDMICS	1			0	0	
BTG	8/20/1997	980459	9708-0016	19,496		Product	Internal, San Antonio	1			0	0	
STK	8/20/1997	51518	9708-0017	16,244		Product	STK, Canada	1			1	0	
BTG	8/20/1997	I980003	9708-0018	32,369		Product	AFIWC	1			1	0	X
Amex	8/31/1997	PHX080309	9708-0024	57,189		Product	Amex	2			0	0	X
Amex	8/31/1997	PHX080314	9708-0025	27,555	193,843	Product	Amex	1			0	0	
								8			3	0	
NGC	8/15/1997		9708-0003	50,000	50,000	Royalty							

EXHIBIT-C-4

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 34 of 109

Wheelgroup Corporation		The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..													
Sales By Category and Month															
	Invoice				Category				NSX		DEV			
Customer	Date	P.O. #	Invoice	Dollars	Total	Category	End User	P	S	MGT	Dlr	SAP	Mnt
Northern Telecom	8/14/1997		9708-0004	11,500		Consulting	Northern Telecom						
Niagara Mohawk	8/14/1997	CC85336AWA	9708-0005	39,050		Consulting	Niagara Mohawk						
AIM Advisors	8/14/1997		9708-0006	10,950		Consulting	AIM Advisors						
Enron	8/14/1997		9708-0013	18,750		Consulting	Enron						
STK	8/29/1997		9708-0023	24,000	104,250	Consulting	National Australia Group						
AT&T	8/21/1997	H3382269	9708-0019	6,475		Training	AT&T						
IBM	8/21/1997	2000379323	9708-0020	1,295		Training	IBM						
STK	8/21/1997		9708-0021	648		Training	STK						
IBM	8/21/1997	2000379323	9708-0022	2,590		Training	IBM						
BTG	8/31/1997	SE980295	9708-0026	3,108	14,116	Training	BTG						
				371,728	371,728								
BTG	9/10/1997	I980008	9709-0005	600	600	Install	BTG						
NetSolve	9/15/1997	M-5461	9709-0007	2,700		Maintenance	Corinthian						
STK	9/30/1997		9709-0014	2,775		Maintenance	STK						
BTG	9/30/1997	980871	9709-0035	17,626	23,101	Maintenance	BTG						
NetSolve	9/1/1997		9709-0001	2,913	2,913	Monitoring	NetSolve						
STK	9/9/1997	51511	9709-0003	12,997		Product	AT&T		1	PP			
STK	9/11/1997	51572	9709-0006	9,156		Product	Allstate Insurance				1	1	
STK	9/23/1997	51581	9709-0012	34,433		Product	Chrysler		1	PP	1	1	
STK	9/23/1997	51559	9709-0018	28,588		Product	Proctor & Gamble	2		CH, BG	1	1	
STK	9/23/1997	51582	9709-0019	25,339		Product	Allstate Insurance		1	PP			
STK-Teris	9/23/1997	JD1-1624-03	9709-0020	70,176		Product	AT&T			PP	1	1	
BTG	9/23/1997	SE980372	9709-0021	27,511		Product	STK-TCG-Federal Region		1	PP	1	1	X
STK-Teris	9/23/1997	JD1-1625-03	9709-0022	22,091		Product	AT&T			PP	1	1	
PEROT	9/23/1997	DMZ-082597	9709-0023	31,352		Product	PEROT		1	CH	1	1	X
BTG	9/23/1997	I980006	9709-0024	136,472		Product	609th IWS	7		BG			X
GRAY PEAK	9/25/1997	1575	9709-0026	23,780		Product	GRAY PEAK	2		CL	1	1	
STK	9/25/1997	51571	9709-0027	18,841		Product	STK, Mississauga	1		BG	1	1	
STK	9/30/1997	51605	9709-0032	9,747		Product	Netsolve - Mirage resorts	1		BG			
STK	9/30/1997	51604	9709-0033	16,244		Product	STK-France	1		BG	1		
BTG	9/30/1997	SE980371	9709-0034	18,219		Product	DMC Denver	1		PP	1		
STK	9/30/1997	51570	9709-0036	19,494		Product	STK, Germany			PP	1		
STK	9/30/1997	51551	9709-0037	12,997		Product	Netcom, Liberty Life-S. Africa			PP			
STK	9/30/1997	51606	9709-0039	48,085		Product	STK, U.K.		3	PP	1	1	
IBM	9/30/1997	2000431615	9709-0040	63,160		Product	IBM	4		CL,BG			X
MLC	9/30/1997	980870	9709-0044	88,477		Product	MLC	4		BG	1	1	
JOHNS HOPKINS	9/30/1997		9709-0045	5,000	722,159	Product	JOHNS HOPKINS						
								23	8		14	11	
NETWORK GENERAL	9/25/1997		9709-0025	50,000	50,000	Royalty	NETWORK GENERAL						
FIRST UNION	9/10/1997		9709-0004	59,600		Consulting	FIRST UNION						
MET	9/15/1997		9709-0008	28,400		Consulting	Met MOA						
E&Y Houston	9/15/1997		9709-0009	47,000		Consulting	Gulf States Toyota						
PICTET	9/15/1997		9709-0010	900		Consulting	PICTET						
JOHNS HOPKINS	9/22/1997		9709-0015	60,000		Consulting	JOHNS HOPKINS						
SHELL PIPELINE	9/22/1997		9709-0016	16,800		Consulting	SHELL PIPELINE						
FEDEX	9/22/1997		9709-0017	42,800		Consulting	FEDEX						
ENRON	9/30/1997		9709-0041	49,000	304,500	Consulting	ENRON						

EXHIBIT-C-5

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 35 of 109

Wheelgroup Corporation			The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..												
Sales By Category and Month															
										NSX		DEV			
Customer	Invoice Date	P.O. #	Invoice	Dollars	Category Total	Category	End User	P	S	MGT	Dir	SAP	Mat
IBM - ERS	9/5/1997	2000400149	9709-0002	20,000	20,000	Support	IBM - ERS						
IBM	9/25/1997	2000379323	9709-0028	6,475		Training	IBM						
AMEX	9/25/1997	PHX130388	9709-0029	2,590		Training	AMEX						
MCNC	9/30/1997	37377	9709-0042	648		Training	MCNC						
BTG	9/30/1997	SE980377	9709-0043	2,072	11,785	Training	BTG						
Total Sept. 1997				**1,135,058**	**1,135,058**								
Total Q3 1997				**1,957,921**	**1,957,921**			**47**	**8**		**27**	**19**	
Netsolve	10/1/1997		9710-0003	3,133	3,133	Monitoring							
STK	10/2/1997	51626	9710-0002	62		Product	STK						
Ernst & Young	10/1/1997	1	9710-0010	25,402		Product	E&Y	1		BG	1	1	X
Network General	10/13/1997	82437	9710-0011	19,788		Product	Network General	1			1		
STK	10/15/1997	51629	9710-0013	9,747		Product	STK, U.K.	1		BG			
MCNC	10/22/1997	37615	9710-0015	42,259		Product	Hory Telephone	2		BG	1	1	X
Interactive Futures	10/22/1997	9221	9710-0016	32,556		Product	N2K		1	CL	1	1	X
BTG	10/22/1997	SE980409	9710-0017	49,630		Product	Joint Chiefs of Staff	2		BG	2	2	X
BTG	10/22/1997	SE980408	9710-0018	113,940		Product	Navy	10		BG			
STK	10/28/1997	51677	9710-0019	22,091		Product	America-On-Line		1	CH	1	1	
STK	10/28/1997	51661	9710-0020	6,497		Product	Boeing				1		
STK	10/28/1997	51665	9710-0021	32,308		Product	Compuserv		1	PP	1	1	
STK	10/23/1997	51672	9710-0024	31,086		Product	Hewlett Packard		1	CH	1	1	
STK	10/27/1997	51673	9710-0025	13,744		Product	STK, UAE	1		BG	1		
NetSolve	10/31/1997		9710-0032	2,720	401,830	Product	Corinthian	1					
								19	4		11	8	
Enron	10/6/1997		9710-0004	16,000		Consulting							
Diamond Shamrock	10/15/1997		9710-0006	22,400		Consulting							
Womble & Carlisle	10/15/1997		9710-0007	9,600		Consulting							
Intrust Bank	10/21/1997		9710-0014	45,000	93,000	Consulting							
Network General	10/1/1997	86414	9710-0012	2,590		Training							
STK	10/9/1997		9710-0026	1,295		Training							
BMC	10/23/1997	9708411	9710-0027	1,295		Training							
Ernst & Young	10/23/1997	DOB922-1	9710-0028	1,295		Training							
STK	10/23/1997	JD1-NR-TRN1	9710-0029	2,590		Training							
Arrow Electronics	10/30/1997		9710-0030	1,295	10,360	Training							
Total Oct 1997					508,323			19	4	0	11	8	
Netsolve	11/24/1997		9711-0001	6,616		Monitoring	NetSolve						
BTG	11/12/1997		9711-0012	23,580		Product	NSA (sold by STK)	1			1		X
BTG	11/30/1997		9711-0019	27,180		Product	NSA (sold by STK)	2					X
IBM - ERS	11/30/1997		9711-0017	66,154		Product	IBM		3				X
IBM - ERS	11/30/1997		9711-0018	107,315		Product	IBM	8					X
STK	11/4/1997		9711-0003	18,841		Product	STK - Sweden		1		1	1	
STK	11/4/1997		9711-0004	22,091		Product	Pilot Network Svc		1		1	1	
STK	11/17/1997		9711-0013	18,841		Product	Bank of America	1			1		
STK	11/18/1997		9711-0010	39,026	323,027	Product	BellSouth Telecomm	3			1	1	
Network General Corporation	11/24/1997		9711-0014	50,000	50,000	Royalty							
Federal Home Loan Bank Dallas	11/10/1997		9711-0002	44,821		Consulting	FHLB						
Harris Publishing Co.	11/26/1997		9711-0016	7,200		Consulting							
U.S. West Communications	11/24/1997		9711-0015	45,000	97,021	Consulting							
Ernst & Young, LLP	11/20/1997		9711-0008	1,295		Training	Ernst & Young, LLP						

EXHIBIT-C-6

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 36 of 109

Wheelgroup Corporation			The below numbers will differ from periodic financial revenue due to accounting adjustments for accruals, etc..												
Sales By Category and Month															
	Invoice					Category				NSX		DEV			
Customer	Date	P.O. #	Invoice	Dollars	Category Total	Category	End User	P	S	MGT	Dir	SAP	Mnt		
Fleet IWC	11/24/1997		9711-0006	1,295		Training	Fleet IWC								
Gray Peak Technologies, Inc.	11/20/1997		9711-0009	648		Training	Gray Peak								
Perot Sytems	11/6/1997		9711-0005	648		Training	Perot Sytems								
STK	11/20/1997		9711-0007	648	4,533	Training	STK								
Total Nov 1997					481,197			15	5	0	5	3			
Alcatel Network Svcs	12/12/1997		9712-0002	35,984		Product	Alcatel Network Svcs	2			1	1	X		
BTG	12/31/1997	SE980533	Note 1	17,080		Product	US Navy		1				X		
BTG	12/5/1997		9712-0010	7,687		Product	NSA (sold by STK)				1		X		
Cemex Central S.A.	12/15/1997		9712-0005	10,328		Consulting	Cemex Central S.A.								
CompuServ Network Svcs	12/1/1997		9712-0003	3,885		Training	CompuServ Network Svcs								
Enron Corp	12/15/1997		9712-0004	51,658		Consulting	Enron Corp								
Horry Telephone Cooperative	12/4/1997		9712-0009	8,571		Product	Horry Telephone Cooperative								
Hucom	12/30/1997		Prepay	900,000		Product									
Network General Corporaton	12/15/1997		9712-0007	50,000		Royalty	Network General Corporaton								
Niagara Mohawk Power	12/18/1997		9712-0008	38,800		Consulting	Niagara Mohawk Power								
Niagara Mohawk Power	12/22/1997	SJ87620AJB	9712-0012	51,720		Product	Niagara Mohawk Power		2		1	1			
Niagara Mohawk Power	12/31/1997	SJ87620AJB	9712-0012	8,045		Training	Niagara Mohawk Power								
Omnipoint Communications	12/31/1997	97115425	Note 1	15,590		Product	Omnipoint								
Omnipoint Communications	12/31/1997	97115426	Note 1	21,985		Product	Omnipoint	1	1						
Omnipoint Communications	12/31/1997	97115427	Note 1	5,629		Product	Omnipoint						X		
Shell Oil Company	12/5/1997		9712-0001	33,600		Consulting	Shell Oil Company								
SmithKline Beecham	12/31/1997	1064962	Note 1	13,570		Product	SmithKline Beecham	1		None			X		
SmithKline Beecham	12/31/1997	1061411	Note 1	23,031		Product	SmithKline Beecham				1	1	X		
STK	12/4/1997		9712-0011	61,220		Product	First Data Resources	4			1				
STK	12/15/1997		9712-0006	22,055		Maint	STK								
STK	12/31/1997	51822	Note 1	27,133		Product	Chrysler Corp		1		1	1			
STK	12/31/1997	51818	Note 1	31,978		Product	Charles Schwab	2			1				
STK	12/31/1997	51825	Note 1	7,694		Product	US West Communication				1	1			
STK	12/31/1997	51784	Note 1	27,884		Product	Allstate Insurnce		1						
STK	12/31/1997	51788	Note 1	16,841		Product	First Union Nat'l Bank	1			1				
STK	12/31/1997	51795	Note 1	16,291		Product	STK - Netherlands	1			1				
STK	12/31/1997	51787	Note 1	10,794		Product	STK - Canada	1							
STK	12/31/1997	51714	Note 1	10,444		Product	STK - Canada		1						
STK	12/31/1997	51682-1	Note 1	32,491		Product	IBM		2		1				
STK	12/31/1997	51715	Note 1	10,444		Product	STK - Canada		1						
STK	12/31/1997	51815	Note 1	13,191		Product	Hiway Technologies	1			1				
STK	12/31/1997	51830	Note 1	10,794		Product	US West Communication								
Texas Instruments	12/31/1997	P301678432	Note 1	82,104		Product	Texas Instruments	10	1		1				
Total Dec 1997					1,678,521										
Total Q4 1997				2,668,040				24	11	0	13	5			
Total 1997				6,489,989				144	19	0	77	39			
Total from Inception								182	19	0	86	39			
Grand Total of NetRanger & Directors								287							

EXHIBIT-C-7

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 37 of 109

Wheelgroup Corporation
Sales By Category and Month
As of 1/5/98

Customer	Category	End User	Fortune 500
CyberSafe Corp.	ICR	CyberSafe Corp.	
AIM Advisors	Consulting	AIM Advisors	
STK	Consulting	AT&T	X
BTG	Consulting	Briefings (Fields, Mony, Navy, etc)	
BTG	Consulting	BTG	
STK	Consulting	Calif. Brd Equal.-Net 'Vest.	
Cemex	Consulting	Cemex	
Cemex Central S.A.	Consulting	Cemex Central S.A.	
CyberSafe Corporation	Consulting	CyberSafe Corp.	
Deloitte & Touche	Consulting	Deloitte & Touche	
Diamond Shamrock	Consulting	Diamond Shamrock	X
Enron Corp	Consulting	Enron Corp	X
FEDEX	Consulting	FEDEX	X
Federal Home Loan Bank Dallas	Consulting	FHLB	X
BTG	Consulting	Fiesta Crow,DARPA, etc.	
FIRST UNION	Consulting	FIRST UNION	X
E&Y Houston	Consulting	Gulf States Toyota	
Harris Publishing Co.	Consulting	Harris Publishing Co.	
IBM ISSC	Consulting	IBM	X
Intrust Bank	Consulting	Intrust Bank	
Guidry	Consulting	Iridium	
JOHNS HOPKINS	Consulting	JOHNS HOPKINS	
LVH	Consulting	LVH	
Lyondell Petrochemical	Consulting	Lyondell	X
MET	Consulting	Met MOA	
STK	Consulting	National Australia Group	
NetSolve	Consulting	NetSolve	
STK	Consulting	Net'Vest - Keytronic SPA	
Niagara Mohawk Power	Consulting	Niagara Mohawk Power	X
Northern Telecom	Consulting	Northern Telecom	
STK	Consulting	NSC SPA	
Openconnect Systems	Consulting	Openconnect Systems	
Origin Systems	Consulting	Origin Systems	
PCL Constructors Inc.	Consulting	PCL	
PICTET	Consulting	PICTET	
Pictet & CIE	Consulting	Pictet & CIE	
CyberSafe Corporation	Consulting	Prudential	
Schrieber	Consulting	Schrieber	
Shell Oil Company	Consulting	Shell Oil Company	
SHELL PIPELINE	Consulting	SHELL PIPELINE	
Sprint	Consulting	Sprint	X
Storage Technology Corp.	Consulting	STK SPA	
Tandem Computers	Consulting	Tandem	
U.S. West Communications	Consulting	U.S. West Communications	X
Womble & Carlisle	Consulting	Womble & Carlisle	

Count			45	11
NetSolve	Mon Serv	BTO		
NetSolve	Mon Serv	CDW		
NetSolve	Mon Serv	Dataworks,CDW,BTO,SMI,GS Toyota, TXI		
BTG	Product	609th IWS		
STK	Product	Aerospace		
BTG	Product	AF - IWS		
BTG	Product	AFIWC		
Alcatel Network Svcs	Product	Alcatel Network Svcs		
STK	Product	All State Insurance		X
STK	Product	America-On-Line		
Amex	Product	Amex		X
BTG	Product	Army JEDMICS		
	Product	Arrow Electronics		X
STK	Product	AT&T		X
STK	Product	Bank of America		
STK	Product	BellSouth Telecomm		X
STK	Product	BMC		
STK	Product	Boeing		X
Netsolve Incorporated	Product	BT Office Supply		
BTG	Product	BTG		
STK	Product	Charles Schwab		
STK	Product	Chrysler		X
STK	Product	Citibank		X
STK	Product	Compuserv		
NetSolve	Product	Computer Disc Warehouse		
Netsolve	Product	Corinthian Schools		
STK	Product	CSE (Canadian equiv. of NSA)		
STK	Product	CSX Technology		X
NetSolve	Product	DataWorks		
BTG	Product	DMC Denver		
Ernst & Young	Product	Ernst & Young		
STK	Product	First Data Resources		X
STK	Product	First Union Nat'l Bank		X
BTG	Product	Ft. Huachuca		
GRAY PEAK	Product	GRAY PEAK		
NetSolve	Product	Gulf States Toyota		
STK	Product	Hewlett Packard		X
STK	Product	Hiway Technologies		
MCNC	Product	Hory Telephone		
Hucom	Product	Hucom		
STK	Product	IBM		X
IBM-ERS	Product	IBM-ERS		
STK	Product	Integrated Data Networks		
JOHNS HOPKINS	Product	JOHNS HOPKINS		

BTG	Product	Joint Chiefs of Staff		
STK	Product	Korea Computer Tech.		
STK	Product	Lockheed		X
MLC	Product	MLC		
STK	Product	Motorola		X
Interactive Futures	Product	N2K		
BTG	Product	Navy		
STK	Product	NetCom Solutions		
NetSolve	Product	NetSolve		
Network General	Product	Network General		
Niagara Mohawk Power	Product	Niagara Mohawk Power		X
BTG	Product	NSA (sold by STK)		
Omnipoint Communications	Product	Omnipoint		
PEROT	Product	PEROT		
STK	Product	Pilot Network Service		
STK	Product	Proctor & Gamble		X
SmithKline Beecham	Product	SmithKline Beecham		
STK	Product	STK		
NetSolve	Product	Structual Metals, Inc.		
NetSolve	Product	Texas Industries		
Texas Instruments	Product	Texas Instruments		X
STK	Product	Unisys		X
BTG	Product	U.S. Navy		
STK	Product	US West Communication		X
			65	20
Grand Total End Users			**111**	**31**

EXHIBIT-C-10

PURCHASE ORDER

BTG INCORPORATED
1945 Old Gallows Road
Vienna, VA 22182
(703) 556-6518
Equal Opportunity Employer

P.O. #: I970035
G/L #: J035-014-51 04

ORDER TO: WHEEL GROUP
13750 SAN PEDRO
SUITE 670
SAN ANTONIO TX 78232

SHIP TO: 1420 KILLIAN AVENUE
SHAW AFB
SC 29152-5029

CONTACT: RICK JORDAN
PHONE: 210-494-3383
FAX: 210-494-6305

DELIVER TO: CAPT. DOUG HARLOW
CONTRACT #: F19628-96-D-0001
PRIORITY: DOA7
F.O.B: DESTINATION

P.O. NO.	P.O. DATE	BUYER	VENDOR NO.	TERMS	SHIP VIA
I970035	07/19/96	CVERCKO, L	WHEEL		BEST WAY

ITEM NUMBER	DESCRIPTION	REQ. DATE	QTY.	UNIT COST	EXT. COST
001.	NETRANGER NSX/2000 (MISC PORTS) PROD. #4871	08/02/96	32.00 /EA	18645.00	596640.00
002.	NETRANGER NSX/2000 ANNUAL SUPPORT & MAINT PROD. #4873	08/02/96	32.00 /EA	3078.0000	98496.00
003.	NETRANGER DIR/SINGLE TIER SOFTWARE V.1.0 PROD. #4875	08/02/96	8.00 /EA	9747.0000	77976.00
004.	NETRANGER DIR ANNUAL SUPT & MAINT PROD. #TBD	08/02/96	8.00 /EA	2279.0000	18232.00
	SUBTOTAL				791,344.00
	SHIPPING				8000.00

NOTES: OVERSHPMTS NOT ACCEPTED

TOTAL 799,344.00

FORM# SELTEK-PO TRANSMITTED IN ELECTRONIC FORMAT BY ST. LUCIE D. [illegible]

EXHIBIT-C-11

Figure 1: NetRanger Communication Architecture

- Flexible
- Fault Tolerant
- Secure
- Scaleable

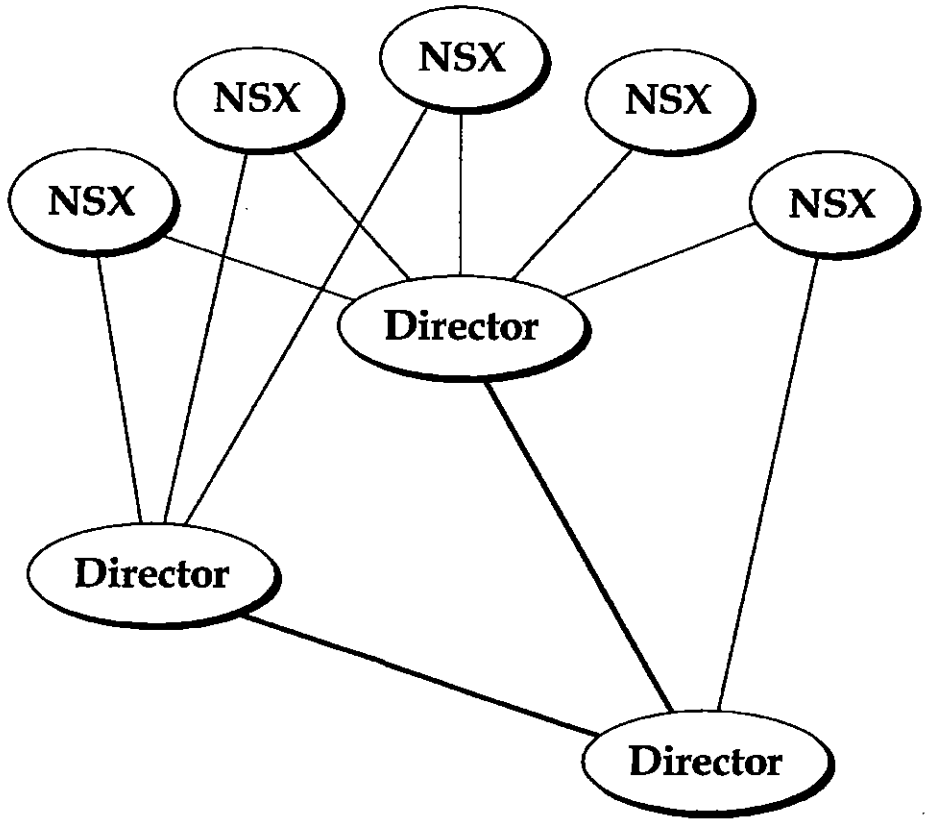


EXHIBIT-D-1

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 43 of 109

Figure 2: NetRanger Hierarchy

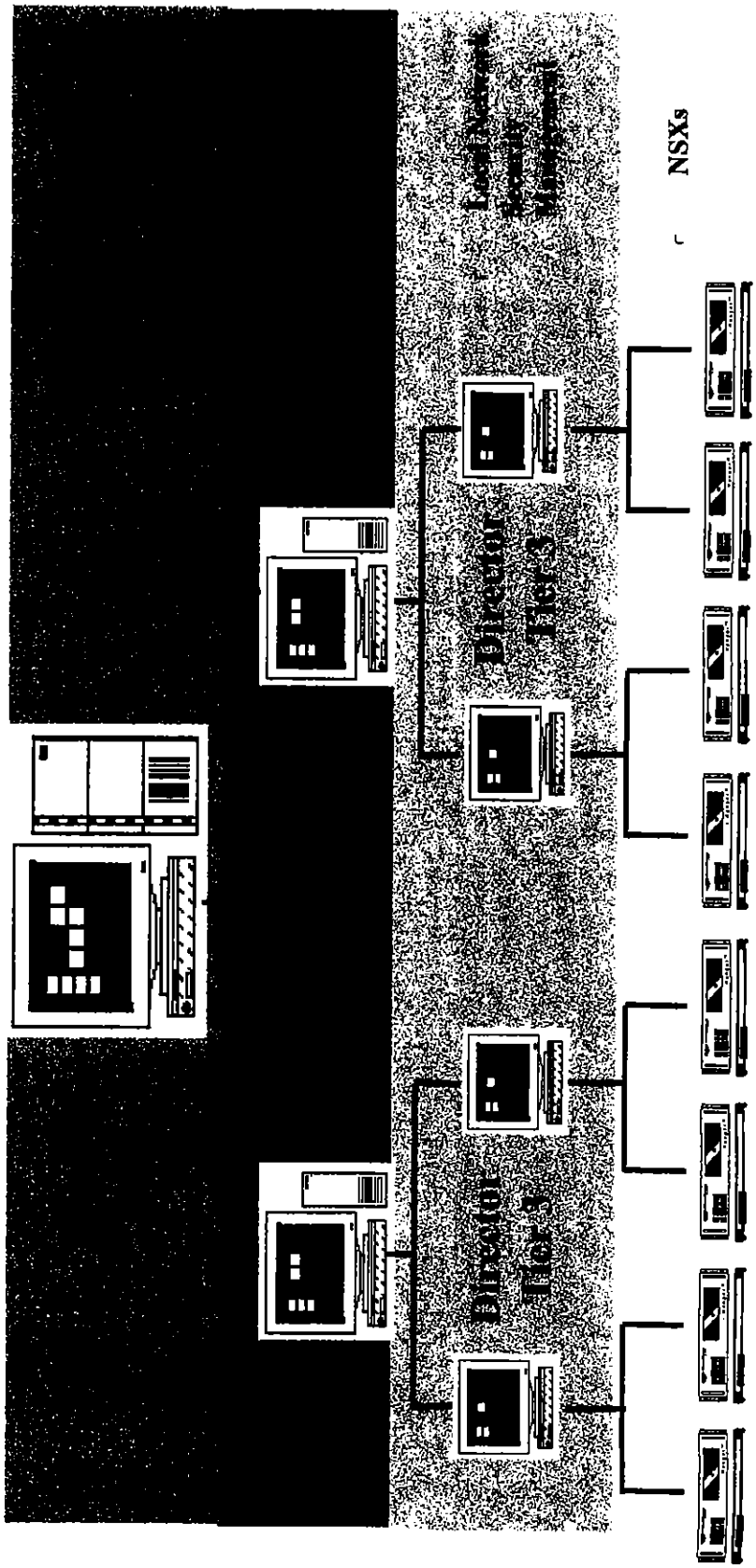


EXHIBIT-D-2

WheelGroup Corporation
"NetRanger"

Both the NetRanger public use or sale and NetRanger User's Guide Version 1.3.1 invalidate the indicated claims under 35 U.S.C. § 102(b) and 103

All text citations for "NetRanger User's Guide Version 1.3.1" are taken from: NetRanger User's Guide Version 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-SYM_P_0075282].

The "NetRanger public use or sale" is based upon the NetRanger software versions 2.0 and earlier. The capabilities of this software are demonstrated in:

Manuals

- NetRanger User's Guide, WheelGroup Corporation, 1996. [SYM_P_0526566-SYM_P_0526735].
- NetRanger High-Level Overview, Version 1.1, WheelGroup Corporation, 11/1996 [SYM_P_0071183- SYM_P_0071199].
- NetRanger User's Guide Version 1.2.2, WheelGroup Corporation, 1997 [SYM_P_0075283- SYM_P_0075535].
- NetRanger User's Guide Version 1.2, WheelGroup Corporation, 1997 [SYM_P_0071736- SYM_P_0071953].
- NetRanger User's Guide Version 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948- SYM_P_0075282].

Government test materials

- "NetRanger Real-Time Network Intrusion Detection Performance and Security Test," DoD/SPOCK, including Appendices A, B and C, 4/30/1997 [SYM_P_0074255-SYM_P_0074481].
- Product Security Assessment of the NetRanger Intrusion Detection Management System Version 1.1, AF Information Warfare Center, 2/1997 [SYM_P_0074527-SYM_P_0074566].

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 46 of 109

WheelGroup Corporation
"NetRanger"

NetRanger code

- NetRanger SQL queries, 5/28/1997 [SYM_P_0074926- SYM_P_0074947].

NetRanger presentations

- NetRanger training slide presentations, 4/1997 [SYM_P_0077338- SYM_P_0077416].

Press / Press Releases

- R. Power and R. Farrow, "Detecting Network Intruders," Network Magazine, pp. 137-38, October 1997 [SYM_P_0078627- SYM_P_0078630].
- PC Week, "NetRanger keeps watch over security leaks," 9/1/97 [SYM_P_0077928- SYM_P_0077931].
- "WheelGroup Releases NetRanger Version 2.0," WheelGroup press release, 8/25/1997 [SYM_P_0074722- SYM_P_0074723].
- "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger Intrusion Detection System," WheelGroup press release, 7/8/1997 [SYM_P_0074647-SYM_P_0074648].
- WheelGroup Press Release Summary [SYM_P_0074525 SYM_P_0074526].

Other documentation

- Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 [SYM_P_0072419- SYM_P_0072641].
- The Security Router Getting Started Guide Release 2.0, NSC, 1995 [SYM_P_0601013-SYM_P_0601752]
- BorderGuard 1000 Reference Manual Release 4.0, NSC, 1996 [SYM_P_0601940-SYM_P_0602441]
- BorderGuard Troubleshooting Guide Release 4.0, NSC, 8/1996 [SYM_P_0602656-SYM_P_0602761]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 47 of 109

WheelGroup Corporation
"NetRanger"

- BorderGuard 1000 Release Notes Release 4.01, NSC, 2/1997 [SYM_P_0601753-SYM_P_0601939]
- NetSentry User Guide Release 4.0, NSC, 2/1997 [SYM_P_0602442-SYM_P_0602655]
- "BorderGuard" by Terry Parsons and Alan Hsu, ZD Internet Magazine, Feb. 1997, http://www.govisionmaster.com/dir_technology/firewalls/15Firewall.htm [SYM_P_0599031].
- BorderGuard Internet Archive documentation [SYM_P_0600799-SYM_P_0600839]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 48 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	"NetRanger is a real-time network security management system that detects, analyzes, responds to, and deters unauthorized network activity. The NetRanger architecture supports large-scale information protection via centralized monitoring and management of remote dynamic packet filtering devices that plug into TCP/IP networks." (1-1) [SYM_P_0074974] "NetRanger enforces an organization's security policy via real-time response and detection of intrusive events without having to erect static barriers. NetRanger's secure communication architecture also allows command and control, as well as system information, to be distributed securely across heterogeneous networks." (1-4) [SYM_P_0074977]	NetRanger was a computer system supporting distributed network security management that comprised: [TS "NetRanger Overview" "Distributed Network Security Management" slide] [DoD p. 2, 4] [SYM_P_0077357, SYM_P_0077367, SYM_P_0074255, SYM_P_0074265]
	deploying a plurality of network monitors in the	See Figure 1.1: Basic NetRanger Components (1-2) [SYM_P_0074975] "The NSX is the sensing and management component of the NetRanger	a plurality of NetRanger sensors ("NSX") deployed in the enterprise network;

[1] The following abbreviations are used to indicate page references:

TS: NetRanger Training slide presentations, 4/1997 [SYM_P_0077338- SYM_P_0077416].

DoD: "NetRanger Real-Time Network Intrusion Detection Performance and Security Test," DoD/SPOCK, 4/30/1997 [SYM_P_0074255- SYM_P_0074481].

SQL: NetRanger SQL queries, 5/28/1997 [SYM_P_0074926- SYM_P_0074947].

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 49 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	enterprise network;	System that resides on a corporate network. It communicates with one or more remote Director systems via the Post Office network communications system. The NSX currently operates with IP networks and supports many hardware and software configuration options. The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor. The Sensor subsystem contains NetRanger's real-time intrusion detection and content assessment logic. The intrusion detection engine recognizes and responds to attacks, such as sendmail, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN scans. Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system. The Sensor also accepts intrusion response and reconfiguration information from the Director systems. ... The Director provides monitoring and analysis services to NetRanger, and communicates with one or more NSX systems via the communication system." (1-2 – 1-3) [SYM_P_0074975- SYM_P_0074976] See Figure 1.6: Director Hierarchy Based on Message Propagation (1-13) [SYM_P_0074906]	[TS "NetRanger Overview" "Distributed Network Security Management" slide, "Communication Architecture" slide] [DoD p. 4] [SYM_P_0077357, SYM_P_0077367, SYM_P_0077364, SYM_P_0074265]
	detecting, by the network monitors,	"The Sensor subsystem contains NetRanger's real-time intrusion detection and content assessment logic. The intrusion detection engine recognizes and	NetRanger NSXs detected a "pattern of misuse" where "misuse is defined as suspicious as well as unauthorized activity"

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 50 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	suspicious network activity	responds to attacks, such as sendmail, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN scans. Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system." (1-2) [SYM_P_0074975] "Although NetRanger is frequently described as an Intrusion Detection system, it also looks for a variety of suspicious activities that precede unauthorized events. An NSX will detect and report a ping sweep of a network. Although not truly intrusive, a ping sweep is frequently a precursor to unauthorized activity. The NSX system therefore looks for network patterns of misuse based on a variety of different attack signatures." (1-5) [SYM_P_0074978] "Attack Signatures As previously mentioned, an attack signature is a pattern of misuse based on one or more events. Such a pattern can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations distributed across multiple hosts over an arbitrary period of time. Events can be grouped into different attack signatures. An event that is based on a single ICMP packet at a specific point in time is an atomic signature (e.g., a ping of a specific host). Composite signatures, on the other hand, are based on series of events. A ping sweep is an example of a signature that spans a network; a port sweep is an example of a signature that focuses on a specific host. A SATAN attack is an example of a composite signature derived from a host port sweep pattern." (1-8) [SYM_P_0074981]	[DoD Appendix A p. 2] [SYM_P_0074298]

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	"The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor. The Sensor subsystem contains NetRanger's real-time intrusion detection and content assessment logic. The intrusion detection engine recognizes and responds to attacks, such as sendmail, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN scans. Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system." (1-2) [SYM_P_0074975] "Network Sensing Patterns of misuse are identified by two basic types of network signatures: context and content. Context-based signatures deal with the state of a transmission as defined by the structure of packet headers, and content-based signatures focus on what is being transported – the binary data." (1-6) [SYM_P_0074979] "Attack Signatures As previously mentioned, an attack signature is a pattern of misuse based on one or more events. Such a pattern can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations distributed across multiple hosts over an arbitrary period of time. Events can be grouped into different attack signatures. An event that is based on a	NetRanger detected misuse based on the content of network packets including at least: • network packet data transfer commands • network packet data transfer errors • network packet data volume • network connection requests • network connection denials • error codes included in a network packet [TS: "NetRanger Overview" "NetRanger NSX Alarm Levels" slide; "Operational Overview" slide] [SYM_P_0077357, SYM_P_0077369, SYM_P_007365] [DoD: p. 14 ("Net Ranger detects misuse based on the content of network packets."); Appendix A; Appendix B] [SYM_P_0074275, SYM_P_0074289- SYM_P_0074321, SYM_P_0074322- SYM_P_0074481]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 52 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		single ICMP packet at a specific point in time is an atomic signature (e.g., a ping of a specific host). Composite signatures, on the other hand, are based on series of events. A ping sweep is an example of a signature that spans a network; a port sweep is an example of a signature that focuses on a specific host. A SATAN attack is an example of a composite signature derived from a host port sweep pattern. Many of these patterns are also sequence-independent, which means that the attack signature must be identified regardless of the order or the duration between atomic events. Other signatures, such as SYN attacks, are based on well-defined event sequences." (1-8) [SYM_P_0074961] "An alarm symbol is created whenever an event that exceeds a user-defined threshold is received." (4-10) [SYM_P_0075066] "The following string detects users attempting to FTP the password file. … The following strings are used to detect the username and passwords of users in ftp sessions. These also indicate when directories are created/deleted and when files are GET/PUT." (4-79) [SYM_P_0075135] "The following example shows how to log every HTTP GET on a network." (4-80) [SYM_P_0075136] "IP Fragmentation attack – Detects an attack that exploits a vulnerability in TCP/IP stacks with IP fragments." (4-61) [SYM_P_0075117] "UDP Bomb – This attack may cause a denial-of-service by crashing the	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		target system the UDP bomb is going to. The SubSigID is the difference in bytes between the IP data length and the UDP datagram length." (4-62) [SYM_P_0075118] "ICMP Unreachable… This message is transmitted to a host stating that the intended destination is unreachable for the IP datagram it transmitted. The first 64 bits of the failed datagram is transmitted along with the unreachable message." (4-67) [SYM_P_0075123] "ICMP Parameter Problem on Datagram… This message is transmitted when a datagram header is incorrect. The first 64 bits of the incorrect header is also sent." (4-69) [SYM_P_0075125] "incom1_tfp_failFailed FTP attempt" (4-82) [SYM_P_0075138] "ICMP Flood – Will fire off if the threshold of X ICMP pkts/sec from a single host is exceeded." (4-61) [SYM_P_0075117] "Context-based signatures are based on information passed in the TCP/IP header. … • Large ICMP traffic. Numerous computers are vulnerable to an attack where if you send an ICMP packet with an extremely large data size it will crash the machine. NetRanger blocks and alarms this traffic." (4-63) [SYM_P_0075119] "Large ICMP Traffic… This signature identifies an attacking host that has	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		transmitted a large ICMP packet." (4-71) [SYM_P_0075127] "ICMP Network Sweeps. This attack uses the ICMP protocol to discover which machines are alive on a remote network. This is most often used as the first step of an attack to find potential targets. All three are detected with NetRanger." (4-63) [SYM_P_0075119] "TCP Port Sweep. When targeting a specific machine, a hacker will frequently run a TCP port sweep to get a list of all available services on the remote target." (4-63) [SYM_P_0075119] "UDP Port Scan. When targeting a specific machine, a hacker will frequently run a UDP port sweep to get a list of all available services on the remote target." (4-63) [SYM_P_0075119] "SATAN Scan. This looks for both the normal and heavy SATAN attacks." (4-63) [SYM_P_0075119] "IP Session logs are either continually active or are only written to when a certain event(s) occurs, such as a connection request from a specific IP address..." (1-10) [SYM_P_0074983] • "Half-Open SYN Attack. This attack was recently publicized when it was used to shut down several Internet Service Providers. This attack can crash a machine by overloading it with TCP connection requests that it never closes.	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		• TCP Hijacking. This attack looks for a characteristic of attacks which take over an existing TCP connection." (4-63) [SYM_P_0075119] "TCP Connection Logging...Level 2: Only TCP SYN packets are logged (default). This indicates that the source host has initiated an attempt to establish a TCP connection to the destination host using the TCP ports specified.... Level 3: All TCP, SYN, FIN, and RST packets are logged. The sequence numbers stored in the miscellaneous field provide enough information to determine the number of bytes transferred within a TCP connection." (4-71 – 4-72) [SYM_P_0075127- SYM_P_0075128] "The next four signatures indicate that a user has multiple failed authentication attempts. ... FTP authentication failure...Telnet authentication failure...rlogin authentication failure..." (4-62) [SYM_P_0075118] See also 4-82, C-2, C-3 [SYM_P_0075138, SYM_P_0075213, SYM_P_0075214]	
	generating, by the monitors, reports of said suspicious activity; and	"Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system." (1-2) [SYM_P_0074975] "Alarms are generated by the sensord daemon, and are typically routed to a remote Director system. These notifications can also be routed to multiple Director systems....	NetRanger NSXs generated alarms [DoD: p. 4, 10, 14] [SYM_P_0074265, SYM_P_0074271, SYM_P_0074275] [TS: "NetRanger Overview" "NetRanger NSX Alarm Levels"

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		The NSX system currently supports two types of logging: • Event logs • IP Session logs Alarms represent just one type of event that can be logged by the NSX system. Event logs (examples of which are shown in Figure 1.4) can also contain entries for every command and error that is generated by a user or NetRanger service." (1-9) [SYM_P_0074962] "Note that both Event and IP Session information can be logged locally on an NSX system as well as remotely on Director systems; exactly what information is sent where depends on how each NSX system is configured." (1-11) [SYM_P_0074964] "When a process on a remote NSX machine detects a security violation, a notification (called an "event") is sent from the NSX machine to the Director machine." (4-1) [SYM_P_0075057]	slide] [SYM_P_0077357, SYM_P_0077369]
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	"Improved Alarm Performance The Director has always avoided generating duplicate alarms by scanning the OVwDB before generating an alarm icon. Prior versions of the Director incurred unnecessary processing overhead by unconditionally scanning the OVwDB. The Director now makes sure that the severity level of the alarm equals or exceeds the OpenView display threshold before it scans the OVwDB. Improved Alarm Consolidation Prior to the 1.3 release, the Director generated a separate alarm icon for	The NetRanger Director received and integrated alarms from the plurality of NSXs. [DoD: p. 4, 7, 10-12 (p. 12 "a Director can consolidate duplicate alarms events into a single icon.")] [SYM_P_0074265, SYM_P_0074268, SYM_P_0074271- SYM_P_0074273] [TS: "NetRanger Overview" "NetRanger Director" slide] [SYM_P_0077357, SYM_P_0077370]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 57 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		every source port accessed by a DNS Request and for every src-dst port pair accessed by a TCP Port Sweep. The Director now generates a single alarm icon for each of these types of events. This dramatically reduces icon and OVwDB clutter as well as improving overall performance under load." (vi) "The Director The Director provides monitoring and analysis services to NetRanger, and communicates with one or more NSX systems via the communication system. The Director contains two basic subsystems, the Security Management Interface (SMI) and the Security Analysis Package (SAP). The SMI is a collection of GUIs and tools that help monitor and respond to security events at one or more NSX locations. The SMI integrates with network management applications (such as HP OpenView®). Whereas the SMI is focused primarily on real-time security event management, data analysis is supported by the SAP. The SAP is a set of data analysis tools that analyzes NSX data independently of SMI activities. The SAP consists of three basic components: data collection, data management, and data analysis. Although all components can be easily integrated into an existing SMI platform, WheelGroup recommends that all data be exported onto a separate database server. In this way, the SMI and SAP components can be configured, secured, and tuned independently." (1-3) [SYM_P_0074976] "As noted earlier, the types of information generated by the NSX daemon falls into four basic categories: Events, Commands, Errors, and IP Packets. The /user/nr/etc/destinations file allows you to specify what types of	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		information should be routed to which daemons on which hosts. Table 1.4 shows two different distribution entries. The first entry routes all of the standard Event data to the loggerd service on a Director machine named crusher, and the second entry specifies that only events should be displayed by smid on the riker Director machine...." (1-12) [SYM_P_0074965] "Director System As noted earlier, the NetRanger Director consists of two major subsystems: • Security Management Interface (SMI) • Security Analysis Package (SAP) These two subsystems provide centralized command and control of an organization's security perimeter, which could conceivable encompass hundreds of NSX systems. From a capabilities perspective, these two subsystems provide monitoring, management, data collection, data analysis, and user-defined actions services." (1-14) [SYM_P_0074967] "The Director ensures that the machine and application that generated the event are represented on the graphical map, and then, if the event's severity level exceeds a user-definable threshold, the Director creates an Alarm icon on the map. The color of the Alarm icon is based on the severity of the event." (4-1) [SYM_P_0075057] "Note that ovw and ovwdb are part of OpenView/NetView, nrdirmap, smid, and loggerd are part of the Director, and sensord is part of the NSX. ... nrdirmap looks at the severity level of the event. If the event severity exceeds a user-specified level, then nrdirmap tells ovw to draw an alarm	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		icon." (4-2) [SYM_P_0075058] "The Alarm Consolidation Threshold describes how many identical alarms must be received before the alarms are replaced by a single "Alarm Set" icon. By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm set" icon." (4-17). [SYM_P_0075073]	
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	"The SAP is a set of data analysis tools that analyzes NSX data independently of SMI activities. The SAP consists of three basic components: data collection, data management, and data analysis. Although all components can be easily integrated into an existing SMI platform, WheelGroup recommends that all data be exported onto a separate database server. In this way, the SMI and SAP components can be configured, secured, and tuned independently." (1-3) [SYM_P_0074976] "A SATAN attack is an example of a composite signature derived from a host port sweep pattern." (1-8) [SYM_P_0074981] See Figure 1.12: NSX Data Collection (1-19) [SYM_P_0074992] "NSX Data Analysis The SAP capability also analyzes data. Rather than locking the user into a single tool on the Director machine, this task is better served by 3rd-party tools on a separate Windows platform, such as the IQ Objects® report writer from IQ Software and multi-dimensional analysis tools such as PowerPlay®	NetRanger included SQL database queries to correlate alarms. [DoD: Appendix A pp. 18-19; Appendix B] [SYM_P_0074279-SYM_P_0074315, SYM_P_0074322- SYM_P_0074481] [SQL] [SYM_P_0074926- SYM_P_0074947]

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		from Cognos. Trouble ticketing systems such as Remedy's Action Request System® (ARS) can also be implemented on top of NetRanger's alarm data. As a foundation for custom reports, SAP includes a subsystem called SAPR. This is a set of SQL queries which can be easily customized or integrated into 3rd-party tools. These types of 3rd-party tools can be configured to support ad hoc queries as well as predefined reports. For example, these tools can easily generate reports showing: • All alarms of levels 4 and 5 in the last 30 days, • A graph of Web server activity over the last 24 hours, and • A table of all events in the last 30 days in order of increasing alarm levels." (1-19 – 1-20) [SYM_P_0074992-SYM_P_0074993] "Analysis Once data is loaded into a database, it can be analyzed for patterns and trends. Status reports relating to network activity and vulnerabilities can also be generated. Although any number of third-party tools can generate these types of output, SAP is shipped with a small but comprehensive collection of Oracle SQL*Plus queries that show how event data can be analyzed relative to different perspectives, such as time versus events. These queries are described in SAP Tutorial." (5-3) [SYM_P_0075141] "The actions that can be launched by sapd include… • Batch, which is a version of ARCHIVE that operates in the background and allows sapd to continue evaluating other conditions without	

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		blocking. This action is intended primarily for launching database reports, which can execute in parallel with other actions." (5-10) [SYM_P_0075148] "Analysis sapr As noted in the High Level Overview section, SAP is shipped with a small collection of SQL queries that generate simple columnar reports. These reports are referred to as the SAP Reports, or sapr, and demonstrate how NetRanger intrusion detection data can be viewed from three basic perspectives: Space, Time, and Events.... Imposing these types of hierarchical structures on NetRanger's event data makes it easier to move from high to low levels of detail as well as shift from one perspective to another." (5-12) [SYM_P_0075150] "Database Reports Setup and Customization... To change the scheduling of reports, customize the SAP triggers. ... The actual SQL DML files [ ] can be changed to alter the selection, sorting, summarization, and display of data." (5-22 – 5-24). [SYM_P_0075160- SYM_P_0075162] "Table 5.4 lists the included queries, which serve as the starting points for query building." (5-36) [SYM_P_0074981]	
3	The method of claim 1, wherein integrating further comprises invoking	"Attack Responses The NSX system does one or more of the following things once an attack has been positively identified: • Generate an alarm.	NetRanger automatically shunned a network connection. [DoD: Appendix A spreadsheet page 2 ("Notify off-duty personnel of events" "Run attack and observe email and/or pager

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	countermeasures to a suspected attack.	• Shun the attack. • Log the alarm event." (1-8) [SYM_P_0074981] "Another way of shunning patterns of misuse is to manually reconfigure the BorderGuard or Passport device through the Director system. Shunning is part of a site's security policy that must be carefully reviewed before it is deployed, whether as a set of automatic rules or as a set of guidelines upon which operational staff rely." (1-9) [SYM_P_0074982] "User-Defined Actions In addition to displaying and logging alarm events, the Director can generate user-defined actions via eventd. A typical action might be to generate pager notifications via e-mail messages or feed data onto 3rd-party devices, such as a printer. Support for multiple actions scripts is also provided. While eventd makes no distinction between alarm types and levels, the default action script shipped with this service shows how actions can be triggered based on these criteria." (1-20) [SYM_P_0074993] "To view an ASCII list of the latest events that have been generated for a given application or machine… This will execute a program that parses the log files… looking for all events for the entity selected. Please note that this will include events that may be below the threshold for creating alarms. Also note that this window is dynamically updated as new events come in." (4-24) [SYM_P_0075080] "By default, eventd is shipped with an e-mail notification service. (Please note that many pager systems can be enabled via e-mail notification.)	activation"; Appendix A p. 5-7, 18] [SYM_P_0074293, SYM_P_0074301- SYM_P_0074303, SYM_P_0074314] [TS: "NetRanger Overview" "NetRanger NSX" slide] [SYM_P_0077357, SYM_P_0077368]

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		eventd receives copies of alarms from smid, arranges them into a readable format, and then sends e-mail messages to users based on information stored in configuration files." (4-56) [SYM_P_0075112]	
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	"The SMI is a collection of GUIs and tools that help monitor and respond to security events at one or more NSX locations. The SMI integrates with network management applications (such as HP OpenView®)." (1-3) [SYM_P_0074976] "There is also an application called nrdirmap that serves as the interface between smid and HP OpenView." (1-14) [SYM_P_0074987] "The nrdirmap application uses the OVW API (OpenView Windows Application Programming Interface) to tell the OpenView user interface what security information to present to the user." (1-15) [SYM_P_0074988] "NSX Data Analysis The SAP capability also analyzes data. Rather than locking the user into a single tool on the Director machine, this task is better served by 3rd-party tools on a separate Windows platform, such as the IQ Objects® report writer from IQ Software and multi-dimensional analysis tools such as PowerPlay® from Cognos. Trouble ticketing systems such as Remedy's Action Request System® (ARS) can also be implemented on top of NetRanger's alarm data. As a foundation for custom reports, SAP includes a subsystem called SAPR. This is a set of SQL queries which can be easily customized or integrated into 3rd-party tools.	NetRanger integrated with a standard interface. [DoD: Appendix A p. 14 "the Director has been integrated with HP's OpenView network management system. This provides the Director with an industry standard command and control interface.")] [SYM_P_0074310] [TS: "NetRanger Overview" "Director Platform Specifications (cont.)"] [SYM_P_0077357, SYM_P_0077362-SYM_P_0077363]

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		These types of 3rd-party tools can be configured to support ad hoc queries as well as predefined reports. (1-20) [SYM_P_0074993] "NetSentry-based signatures are generated by reporting packet failures and/or successes from NetSentry filters. When the NSG BorderGuard is used to enforce a specific security policy, an option exists to copy a subset of failed packets from the BorderGuard to the NSX. Each copied packet includes the name of the NetSentry filter that failed the packet.... Using this NetRanger capability, and filter on the BorderGuard is capable of generating event signatures. Because the BorderGuard allows a large number of highly configurable filters using the NetSentry filter language, the number of potential NetSentry event signatures generated by NetRanger could be considered unlimited." (4-81) [SYM_P_0075137]	
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	"The NetRanger architecture supports large-scale information protection via centralized monitoring and management of remote dynamic packet filtering devices that plug into TCP/IP networks." (1-1) [SYM_P_0074974] "The NSX currently operates with IP networks and supports many hardware and software configuration options." (1-2) [SYM_P_0074975] "Network Protocols The sensor subsystem currently works with TCP/IP." (1-6) [SYM_P_0074979]	NetRanger ran in a LAN, WAN, or Internet network. [DoD: p. 2, 3, 5, 9, 10] [SYM_P_0074263, SYM_P_0074264, SYM_P_0074266, SYM_P_0074270, SYM_P_0074271]
6	The method of claim 1, wherein the network monitors	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of	NetRanger NSXs were deployed at routers or proxy servers.

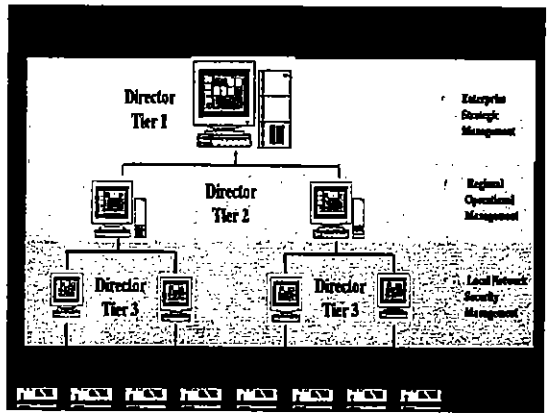
Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 65 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly, • Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections. Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996- SYM_P_0074997] See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009]	[TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357, SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263, SYM_P_0074264]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 66 of 109

WheelGroup Corporation
"NetRanger"

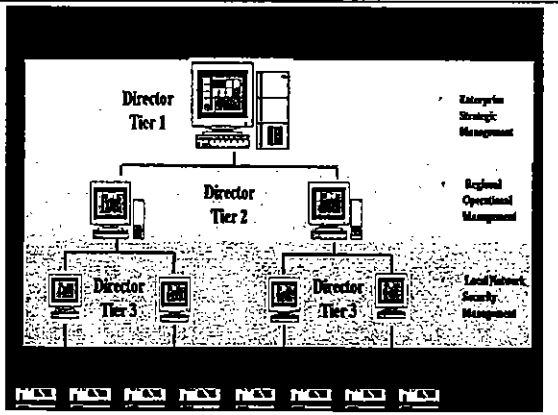
'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		"The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	
7	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	"Distribution Hierarchies Another feature that complements alternate routing is the ability to build hierarchies of NSX and Director systems through the use of message propagation. Instead of broadcasting events from an NSX onto multiple hosts, information can be sent to a single host, which can then propagate packets onto other platforms defined in its local configuration files. Figure 1.6 illustrates this concept via a simple hierarchy of Director machines. In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9AM to 5PM and then transfer control onto a central Director every evening." (1-13) [SYM_P_0074986] See Figure 1.6: Director Hierarchy Based on Message Propagation (1-13) [SYM_P_0074986] "The Director hierarchy includes the following levels, where NetRanger is the "root" and Events/Alarms are the "leaf" nodes of the tree: • NetRanger ▪ Collections of Directors/NSXs • A Single Director or NSX System	A NetRanger Director received and integrated alarms from a plurality of NetRanger NSXs. 

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 67 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		○ Applications running on a Director or NSX System ▪ Events/Alarms generated by an Application" (1-15) [SYM_P_0074988] "NSX Collections are used to customize, or partition, the map. NSX Collections are good tools to use for grouping machines into logical units." (4-14) [SYM_P_0075070] "NSX Collection entities can be used to customize, or partition, a map. If the number of NSX machines you are monitoring is too great to represent on a single submap (for instance, the Top-Level NSX Collection submap), you can create additional Collections, and then add Machine icons to those Collection submaps. This allows you to create a hierarchical grouping of machines." (4-20) [SYM_P_0075070] "You can create customized maps for different users. Each user's map can have a different subset of NSX Machines displayed. ... Usually, Machine symbols are deleted to create a "user domain" with a subset of the configured NSX Machines." (4-41) [SYM_P_0075097]	[DoD: pp. 4, 7; Appendix A, spreadsheet page 1 "Hierarchical Propagation of Alarms"] [SYM_P_0074265, SYM_P_0074268, SYM_P_0074292] [TS: "NetRanger Overview" "Communication Architecture" slide, "Distributed Network Security Management" slide] [SYM_P_0077357, SYM_P_0077364, SYM_P_0077367]
8	The method of claim 7, wherein receiving and integrating is performed by a domain monitor	"Distribution Hierarchies Another feature that complements alternate routing is the ability to build hierarchies of NSX and Director systems through the use of message propagation. Instead of broadcasting events from an NSX onto multiple hosts, information can be sent to a single host, which can then propagate packets onto other platforms defined in its local configuration files. Figure	A NetRanger Director received and integrated alarms from a plurality of NetRanger NSXs.

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	with respect to a plurality of service monitors within the domain monitor's associated network domain.	1.6 illustrates this concept via a simple hierarchy of Director machines. In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9AM to 5PM and then transfer control onto a central Director every evening." (1-13) [SYM_P_0074986] See Figure 1.6: Director Hierarchy Based on Message Propagation (1-13) [SYM_P_0074986] "The Director hierarchy includes the following levels, where NetRanger is the "root" and Events/Alarms are the "leaf" nodes of the tree: • NetRanger ▪ Collections of Directors/NSXs • A Single Director or NSX System o Applications running on a Director or NSX System ▪ Events/Alarms generated by an Application" (1-15) [SYM_P_0074988] "NSX Collections are used to customize, or partition, the map. NSX Collections are good tools to use for grouping machines into logical units." (4-14) [SYM_P_0075070] "NSX Collection entities can be used to customize, or partition, a map. If the number of NSX machines you are monitoring is too great to represent on	 [DoD: pp. 4, 7; Appendix A, spreadsheet page 1 "Hierarchical Propagation of Alarms"] [SYM_P_0074265, SYM_P_0074268, SYM_P_0074292] [TS: "NetRanger Overview" "Communication Architecture" slide, "Distributed Network Security Management" slide] [SYM_P_0077357, SYM_P_0077364, SYM_P_0077367]

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
		a single submap (for instance, the Top-Level NSX Collection submap), you can create additional Collections, and then add Machine icons to those Collection submaps. This allows you to create a hierarchical grouping of machines." (4-20) [SYM_P_0075070] "You can create customized maps for different users. Each user's map can have a different subset of NSX Machines displayed. … Usually, Machine symbols are deleted to create a "user domain" with a subset of the configured NSX Machines." (4-41) [SYM_P_0075097]	
9	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 8	A higher-tier NetRanger Director received and integrated alarms from a plurality of lower-tier NetRanger Directors. See '203 claim 8 [DoD: pp. 4, 7, 19; Appendix A, spreadsheet page 1 "Hierarchical Propagation of Alarms"] [SYM_P_0074300, SYM_P_0074303, SYM_P_0074315, SYM_P_0074292] [TS: "NetRanger Overview" "Communication Architecture" slide, "Distributed Network Security Management" slide] [SYM_P_0077357, SYM_P_007364, SYM_P_0077367]
10	The method of claim 9, wherein	See '203 claim 8	A higher-tier NetRanger Director received and integrated alarms from a plurality of lower-tier NetRanger Directors.

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.		See '203 claim 8 [DoD: pp. 4, 7, 19; Appendix A, spreadsheet page 1 "Hierarchical Propagation of Alarms"] [SYM_P_0074300, SYM_P_0074303, SYM_P_0074315, SYM_P_0074292] [TS: "NetRanger Overview" "Communication Architecture" slide, "Distributed Network Security Management" slide] [SYM_P_0077357, SYM_P_0077364, SYM_P_0077367]
11	The method of claim 9, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	"Distribution Hierarchies Another feature that complements alternate routing is the ability to build hierarchies of NSX and Director systems through the use of message propagation. Instead of broadcasting events from an NSX onto multiple hosts, information can be sent to a single host, which can then propagate packets onto other platforms defined in its local configuration files. Figure 1.6 illustrates this concept via a simple hierarchy of Director machines. In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9AM to 5PM and then transfer control onto a central Director every evening." (1-13) [SYM_P_0074986]	A NetRanger Director communicated with another Director. [DoD p. 1; Appendix A spreadsheet page 1 ("Information can be Propagated Between Directors"); Appendix A p. 13 "A Director can forward alarms to another Director")] [SYM_P_0074292, SYM_P_0074309]
12	An enterprise network monitoring system comprising:	See '203 claim 1	See '203 claim 1
	a plurality of	See '203 claim 1	See '203 claim 1

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 71 of 109

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	network monitors deployed within an enterprise network;		
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	See '203 claim 1	See '203 claim 1
	said network monitors generating	See '203 claim 1	See '203 claim 1

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	reports of said suspicious activity; and		
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 1	See '203 claim 1
13	The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
14	The system of claim 12, wherein the integration further comprises invoking	See '203 claim 3	See '203 claim 3

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	countermeasures to a suspected attack.		
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
17	The system of claim 12, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network:	See '203 claim 6	See '203 claim 6

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	{gateways, routers, proxy servers}.		
18	The system of claim 12, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8 and '203 claim 9	See '203 claim 8 and '203 claim 9
19	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
20	The system of claim	See '203 claim 9	See '203 and 9

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	12, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
21	The system of claim 20, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
22	The system of claim 20, wherein the plurality of domain	See '203 claim 11	See '203 claim 11

WheelGroup Corporation
"NetRanger"

'203 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)[1]
	monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.		

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '203 claim 1 See also: "New Content Signatures… Unknown IP Protocol" (ix) "Unknown IP Protocol – Alarms on any IP packet with a protocol number that RFC1700 declares reserved or unassigned." (4-61) [SYM_P_0075117]	See '203 claim 1 NetRanger detected misuse based on the content of network packets including at least: • network packet data transfer commands • network packet data transfer errors • network packet data volume • network connection requests • network connection denials • error codes included in a network packet • network packets indicative of well-known service protocols
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 78 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly, • Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections.	NetRanger NSXs were deployed at routers or proxy servers. [TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357, SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263,

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 79 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996-SYM_P_0074997] See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009] "The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	SYM_P_0074264]

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	103 [*Emerald 1997; Statistical Methods*]	103 [*Emerald 1997; Statistical Methods*]
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8 and 9
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
12	The method of claim 10, wherein the	See '203 claim 11	See '203 claim 11

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 81 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.		
13	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '615 claim 1	See '615 claim 1
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '615 claim 6	See '615 claim 6
19	The system of claim 13, wherein the plurality of network monitors includes a	See '203 claim 8	See '203 claim 8 and 9

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 83 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	plurality of service monitors among multiple domains of the enterprise network.		
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
23	The system of claim 21, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 84 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly, • Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections. Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996-SYM_P_0074997]	NetRanger NSXs were deployed at routers or proxy servers. [TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357, SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263, SYM_P_0074264]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 85 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009] "The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
35	The method of claim 34, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
36	The method of claim 34, wherein said integrating further comprises invoking	See '203 claim 3	See '203 claim 3

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 86 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	countermeasures to a suspected attack.		
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
39	The method of claim 34, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
41	The method of claim 34, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
42	The method of claim 41, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
43	The method of claim 41, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a router;	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly,	NetRanger NSXs were deployed at routers or proxy servers. [TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357,

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 88 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		• Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections. Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996-SYM_P_0074997] See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009] "The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security	SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263, SYM_P_0074264]

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
46	The method of claim 44, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
48	The method of claim 44, wherein said network traffic data is selected from one or more of the following categories:	See '615 claim 1	See '615 claim 1

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	{network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.		
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
51	The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
52	The method of claim 51, wherein said receiving and integrating is performed by	See '203 claim 10	See '203 claim 10

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.		
53	The method of claim 51, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
64	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a firewall;	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly, • Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections. Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as	NetRanger NSXs were deployed at routers or proxy servers. [TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357, SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263, SYM_P_0074264]

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 92 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996-SYM_P_0074997] See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009] "In cases where there is no need for address translation or other proxy services, NetRanger can replace firewalls. If there is no need for address translation or other proxy services, NetRanger works best without a firewall and has less impact on network performance." (2-3) [SYM_P_0074996] "The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	
	detecting, by the network monitors,	See '615 claim 1	See '615 claim 1

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	suspicious network activity based on analysis of network traffic data;		
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
65	The method of claim 64, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
66	The method of claim 64, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
67	The method of claim 64, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
68	The method of claim 64, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection	See '615 claim 1	See '615 claim 1

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	denials, error codes included in a network packet}.		
69	The method of claim 64, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
70	The method of claim 69, wherein said receiving and integrating is preformed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
71	The method of claim 64, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
72	The method of claim 71, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See'203 claim 10	See'203 claim 10
73	The method of claim 71, wherein the	See '203 claim 11	See '203 claim 11

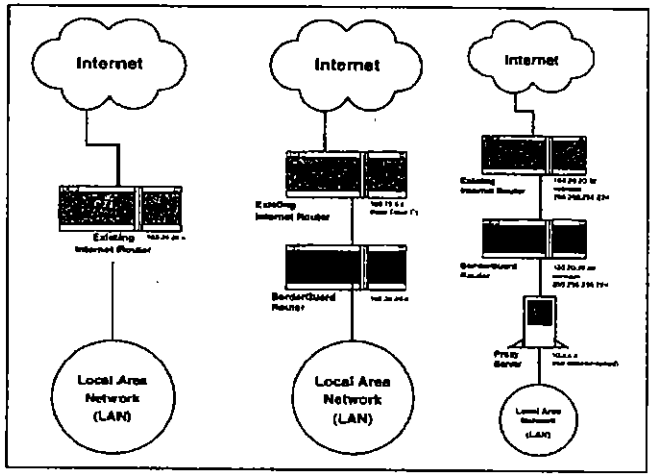
WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.		
84	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network, wherein at least one of the network monitors is deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers, firewalls}, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data;	"The only type of packet filter devices the sensor subsystem currently works with are the BorderGuard and Passport devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system. In addition to serving as high-speed IP data sources, all of these devices • Can be reconfigured on the fly, • Support a common NetSentry interface, • Can be deployed as bridges as well as routers, and • Can maintain Virtual Private Network (VPN) connections. Because these devices can be reconfigured on the fly, NetRanger can dynamically shun as well as detect suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses." (1-6) [SYM_P_0074979] "Please note that when an NSX Sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed." (2-3 – 2-4) [SYM_P_0074996-	NetRanger NSXs were deployed at routers or proxy servers. [TS: "NetRanger Overview" "NSX Configurations" slide "NetRanger Application" slide] [SYM_P_0077357, SYM_P_0077359, SYM_P_0077366] [DoD: pp. 2, 3] [SYM_P_0074263, SYM_P_0074264]

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		SYM_P_0074997] See Figure 2.7: The NSX Sensor Placed on its Own Isolated Network (2-10) [SYM_P_0075003] "WheelGroup recommends that you place the NSX in a secure location and physically close to the BorderGuard with which it will be operating." (3-1) [SYM_P_0075009] "The second option also requires that subnetting the class C address assigned to the BorderGuard router and the proxy server. While both of these options are fairly difficult, obtaining a new address is the least problematic of the two. These options are diagrammed in Figure 2.6." [SYM_P_0075002]	

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 97 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
		 *Figure 2.6: BorderGuard Router Placed Behind the Existing Internet Router* (2-9) [SYM_P_0075002] "The Packet Filtering Device is a router or bridge that plugs into a corporation's network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor." (1-2) [SYM_P_0074975]	

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 98 of 109

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
85	The system of claim 84, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
86	The system of claim 84, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
87	The system of claim 84, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
88	The system of claim 84, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network	See '615 claim 1	See '615 claim 1

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	connection requests, network connection denials, error codes included in a network packet}.		
89	The system of claim 84, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
90	The system of claim 89, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
91	The system of claim 84, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
92	The system of claim 91, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10

WheelGroup Corporation
"NetRanger"

'615 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
93	The system of claim 91, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 101 of 109

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
1	Method for monitoring an enterprise network, said method comprising the steps of:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data,	See '203 claim 1	See '203 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	103 [*Statistical Methods; Emerald 1997*]	103 [*Statistical Methods; Emerald 1997*]
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1,	See '203 claim 1	See '203 claim 1

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 102 of 109

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	wherein at least one of the network monitors utilizes a signature matching detection method.		
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	See '212 claims 1 and 2	See '212 claims 1 and 2
4	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
5	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
6	The method of claim 1, wherein the plurality of network monitors includes an API for encapsulation of monitor functions and integration of third-party	See '203 claim 4	See '203 claim 4

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	tools.		
7	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
8	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '203 claim 6	See '203 claim 6
9	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
10	The method of claim 9, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated	See '203 claim 8	See '203 claim 8

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	network domain.		
11	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
12	The method of claim 11, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
13	The method of claim 11, wherein the plurality of the domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
14	An enterprise network monitoring system	See '212 claim 1	See '212 claim 1

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	comprising:		
	a plurality of network monitors deployed within an enterprise network;	See '212 claim 1	See '212 claim 1
	said plurality of network monitors detecting suspicious network activity	See '212 claim 1	See '212 claim 1
	based on analysis of network traffic data,	See '212 claim 1	See '212 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	See '212 claim 1	See '212 claim 1
	said network monitors generating reports of said suspicious activity; and	See '212 claim 1	See '212 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '212 claim 1	See '212 claim 1
15	The system of claim 14, wherein the integration comprises correlating intrusion reports reflecting	See '203 claim 2	See '203 claim 2

Case 1:04-cv-01199-SLR Document 352-2 Filed 06/30/2006 Page 106 of 109

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	underlying commonalities.		
16	The system of claim 14, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
17	The system of claim 14, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
18	The system of claim 14, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
19	The system of claim 14, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '206 claim 6	See '206 claim 6
20	The system of claim 14,	See '203 claim 7	See '203 claim 7

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.		
21	The system of claim 20, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
22	The system of claim 14, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
23	The system of claim 22,	See '203 claim 10	See '203 claim 10

WheelGroup Corporation
"NetRanger"

'212 Claim number	Claim Term	NetRanger User's Guide Version 1.3.1 (printed publication)	NetRanger (public use or sale)
	wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.		
24	The system of claim 22, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11